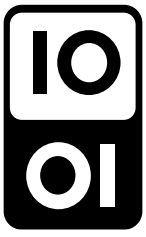
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉDUCATION
NATIONALE ET
DE LA JEUNESSE

CARMO

Cadre de référence pour l'Accès aux Ressources pédagogiques via un équipement Mobile

POUR L'ÉCOLE
DE LA CONFIANCE



Version 3.0 – décembre 2018

Table des matières

Table des illustrations

Liste des tableaux

1. Préambule

Les investissements des collectivités territoriales et de l'État pour le numérique éducatif se sont structurés autour de projets d'équipements et de services numériques (matériels individuels pour les élèves et leurs enseignants, collectifs pour les établissements, câblages, raccordements à internet, espaces numériques de travail (ENT), ressources numériques et formation) intégrant un accompagnement dans les établissements scolaires.

La mise à disposition de ressources numériques via des supports mobiles dans un environnement de confiance, adapté à l'usage dans l'éducation, est positionnée au cœur de la stratégie du ministère de l'éducation nationale et de la jeunesse, qui coordonne un programme d'accompagnement des projets numériques dans les territoires.

Les retours d'expérience, en France mais également à l'étranger, font état d'une complexité de mise en œuvre. Les projets d'équipements pour l'accès aux ressources pédagogiques nécessitent en effet une approche globale et la prise en compte d'un environnement technologique et humain.

Plusieurs conditions sont à réunir pour garantir un retour sur investissement d'un point de vue éducatif et pédagogique : l'accompagnement de proximité et la formation des enseignants, des conseillers pédagogiques, chefs d'établissement et corps d'inspection ; le renforcement de la gouvernance partagée entre État et collectivités territoriales ; les garanties pour la protection des données à caractère personnel et la liberté pédagogique des enseignants, ainsi qu'un cadre national pour partager les objectifs et guider les projets territoriaux.

Le présent document est au service des relations État-Collectivités en fournissant un cadre de référence pour l'élaboration et la mise en œuvre des projets d'équipements mobiles pour l'accès aux ressources pédagogiques numériques.

Document évolutif, ce cadre de référence constitue également un instrument de dialogue, d'une part entre l'éducation nationale et ses partenaires, d'autre part au sein même des différents services et entités de l'éducation nationale et enfin, avec les acteurs de la filière industrielle.

2. Concepts fondamentaux

Pour utiliser les ressources numériques (contenus et services) nécessaires aux apprentissages, les membres de la communauté éducative ont besoin d'accéder via un équipement mobile (EM) à ces ressources, qu'elles servent à des activités pédagogiques personnalisées ou à des pratiques collaboratives et partagées.

L'équipement mobile désigne un terminal informatique répondant à des besoins d'usages nomades.

Dans le présent document, les projets qui ont pour finalité de permettre à la communauté éducative des écoles, collèges et lycées, d'accéder aux ressources pédagogiques via des équipements mobiles seront nommés « projets d'équipements mobiles ». Ces projets peuvent faire le choix :

- d'acquérir des équipements mobiles et de les mettre à disposition des élèves et enseignants, de façon individuelle et avec possibilité pour eux de les ramener à la maison ; dans ce cas, ils seront désignés dans le présent document par le terme « EIM » - pour équipement individuel mobile ;
- d'acquérir des dispositifs de type « classe mobile » et d'attribuer collectivement (par classe ou établissement) voire individuellement les équipements mobiles qui les composent ; cela peut tendre à de l'équipement individuel mais dans l'établissement uniquement ;
- de soutenir et accompagner l'utilisation (voire l'acquisition) d'équipements mobiles appartenant aux utilisateurs et dont la responsabilité ne relève ni de l'État ni de la collectivité ; dans ce cas, ils sont qualifiés d'équipements BYOD/AVEC[1].

  Les terminaux BYOD/AVEC représentent un cas particulier des équipements individuels mobiles et seuls certains aspects de leur mise en œuvre sont évoqués dans ce cadre de référence ; davantage de détails figurent dans le « Guide des projets pédagogiques s'appuyant sur le BYOD/AVEC ».

Un équipement mobile dans l'éducation doit permettre d'accéder au bouquet de ressources (contenus et services) spécifiquement prévu pour la communauté de l'établissement scolaire. Le cas échéant, le projet doit fournir à l'enseignant les outils d'organisation et d'animation pour mettre les équipements mobiles de ses élèves au service de ses pratiques pédagogiques (c'est notamment le cas lorsqu'il s'agit d'un projet de type EIM).

> Les caractéristiques d'un équipement mobile sont détaillées dans le chapitre 7.
>
> Les services fonctionnels et fonctionnalités principales de « gestion de classe » sont détaillés dans le chapitre 17.
>
> Les fonctionnalités de distribution des applications mobiles sont décrites dans le chapitre 13.
>
> Les recommandations pour les dispositifs de type « classe mobile » sont indiquées au chapitre 19.

La mise à disposition d'équipements mobiles dans un établissement scolaire nécessite la mise en place d'outils de gestion de flotte ainsi qu'une intégration au système d'information existant.

> Les caractéristiques attendues d'une solution de gestion de flotte dans l'éducation sont décrites dans le chapitre 12.
>
> La liste des services d'infrastructures pour l'établissement et de gestion du stockage sont respectivement présentés dans les chapitres 15 et 16.

La réussite du déploiement et de la mise en œuvre des équipements mobiles dans les établissements nécessite la mise en place d'une organisation projet, inscrite dans une logique partenariale État-Collectivités territoriales. Pour servir les finalités éducatives, le projet d'équipement mobile doit permettre de garantir un cadre de confiance, respectueux du cadre juridique, des exigences de sécurité et des règles de gestion des données à caractère personnel et notamment des règles issues du Règlement (UE) 2016/679 général relatif à la protection des données (RGPD) et de la loi n°78-17 Informatique et Libertés du 6 janvier 1978 modifiée en 2018.

[1] À consulter le Guide des projets pédagogiques s'appuyant sur le BYOD/AVEC version V1.2 (eduscol.education.fr/cid128686/guide-des-projets-pedagogiques-s-appuyant-sur-le-byod-avec.html). Dans la suite du texte, on se limitera au seul acronyme « BYOD » pour désigner « BYOD/AVEC » hormis pour citer ce guide.

Les exigences de sécurité sont décrites dans le chapitre 14.

La loi n° 2018-771 du 5 septembre 2018 pour la liberté de choisir son avenir professionnel et la loi d'orientation et de programmation pour la refondation de l'École de la République du 8 juillet 2013 ont permis des avancées majeures dans la politique de scolarisation des élèves en situation de handicap. L'école est une chance et un droit auxquels tous les enfants peuvent prétendre, et ces lois en réaffirment les principes d'accessibilité (accès à tout pour tous) et de compensation (mesures individuelles rétablissant l'égalité des droits et des chances). L'usage du numérique (équipement et ressources) est une réelle opportunité pour faciliter la prise en compte de besoins éducatifs particuliers.

Le document liste un ensemble d'illustrations sur l'apport du numérique aux personnes en situation de handicap, et de recommandations pour que ces possibilités soient bien prises en compte. Ces rappels sur l'accessibilité ne donnent pas lieu à un chapitre particulier mais sont inclus au fil du document.

3. Objectifs, cibles et statut du cadre de référence (CARMO)

3.1. Objectifs du document

Le présent document a pour objectif de fournir le **C**adre de référence national pour l'**A**ccès aux **R**essources pédagogiques via un équipement **Mo**bile (CARMO).

Il vise à fournir :

- les grandes orientations pour la mise en œuvre des projets d'équipements mobiles à destination des membres de la communauté éducative de l'établissement (en particulier les élèves et leurs enseignants) ; ces orientations sont issues d'une démarche concertée État-Collectivités pour le service public du numérique éducatif ;
- les recommandations principales pour élaborer et conduire les projets ; ces recommandations sont détaillées afin d'aider les porteurs de projet dans l'élaboration de leurs cahiers des charges et l'organisation du projet, et d'aider les acteurs de la filière industrielle en leur présentant les attentes pour le numérique éducatif.

3.2. Statut du document

Les orientations du cadre de référence CARMO concernent les points jugés par l'éducation nationale et ses partenaires comme suffisamment importants et structurants pour être portés à l'attention des destinataires du présent document.

Les recommandations fournies deviendront une obligation par le biais des contrats, issus des marchés publics conclus entre les collectivités territoriales et les prestataires (constructeurs, fournisseurs de services, intégrateurs, hébergeurs ou encore infogérants) ainsi que par le biais des conventions, notamment celles établies entre les services académiques et les collectivités.

En outre, le document identifie parmi ces recommandations celles qui sont jugées comme indispensables pour garantir la conformité au contexte éducatif (missions éducatives, finalités d'usages, respect des contraintes réglementaires, juridiques et de sécurité). Elles sont repérables par les verbes « **DOIT** » ou « **DOIVENT** ».

Le présent document constitue la troisième version du cadre de référence CARMO et présente les évolutions suivantes par rapport à la version 2 publiée en juin 2016 :

- des précisions sur l'alimentation en données des solutions de gestion de flotte (MxM) / gestion de classe ;
- le lien avec le « Guide des projets pédagogiques s'appuyant sur le BYOD/AVEC » ;
- l'adaptation à l'évolution des dispositions relatives à la protection de données à caractère personnel ;
- les liens entre ENT et les équipements mobiles et l'alignement avec d'autres référentiels tels que CARINE ;
- la prise en compte de l'évolution de la terminologie et du contexte stratégique et réglementaire ;
- l'amélioration de l'accessibilité du document.

Compte tenu de leur maturité à l'échéance de publication du présent document (décembre 2018), certains sujets n'ont pas été traités dans cette version et feront l'objet de publications ultérieures. C'est notamment le cas pour :

- le détail des normes et standards pour les ressources et applications mobiles ;

- les liens avec les projets nationaux pour l'environnement numérique de confiance (en particulier le GAR - gestionnaire d'accès aux ressources - et le mécanisme d'identification FranceConnect) ;
- les opérations de transition d'année scolaire.

3.3. Destinataires du document

Le cadre de référence CARMO vise à faciliter le dialogue entre les acteurs pour la mise en œuvre des projets d'équipements mobiles.

Les principaux acteurs de ces projets sont :

- les ministères (services centraux) :
  - Ministère de l'Éducation nationale et de la jeunesse (MENJ) : il coordonne les travaux pour la formalisation des grandes orientations et des recommandations, au service de la politique nationale d'éducation et dans le cadre de la stratégie numérique pour la refondation de l'école,
  - Ministère de l'Économie, de l'Industrie et du Numérique (MEIN) : il impulse le développement et la structuration de la filière industrielle française du numérique éducatif, avec des enjeux de souveraineté nationale et de création d'emplois qualifiés,
  - Ministère de l'Agriculture et de l'Alimentation (MAA) : il inscrit sa participation au service public du numérique éducatif et de l'enseignement à distance et dans ce cadre il contribue à la définition des besoins métier et des recommandations, afin que les projets territoriaux faisant le choix d'équiper les établissements d'enseignement agricole puissent bénéficier de définitions et d'orientations convergentes ;
- les associations représentatives des collectivités territoriales : une concertation au niveau national permet de partager les objectifs et préparer les orientations (notamment par le biais du « comité des partenaires ») ;
- le Secrétariat général pour l'investissement (SGPI) : il soutient, par le biais du Programme d'Investissement d'Avenir, les projets numériques pour l'éducation des collectivités territoriales ainsi que le développement de l'environnement d'accès aux ressources.
- les maîtrises d'ouvrage académiques et territoriales (« porteurs de projet ») : elles définissent le besoin, pilotent le projet et financent la mise en œuvre, avec un intérêt particulier porté aux questions de sécurité ;
- les chefs d'établissement et directeurs d'école : ils définissent et mettent en œuvre les projets pédagogiques ;
- les personnes ressources en établissement (en particulier « administrateurs ») ;
- les délégués à la protection des données (DPD) ;
- les enseignants ;
- les représentants des parents d'élèves ;
- les acteurs de la filière industrielle :
  - fabricants de matériel,
  - fournisseurs de solutions applicatives (de gestion de flotte mobile, de bouquets de service, de sécurité, de gestion de classe…),
  - fournisseurs de ressources pédagogiques (contenus et services),
  - prestataires des maîtrises d'ouvrage académiques et territoriales ;
- les acteurs et personnes concernés par l'assistance aux élèves en situation de handicap :
  - assistants de vie scolaire (AVS) et accompagnants des élèves en situation de handicap (AESH),
  - ergothérapeutes,
  - psychologues,

- orthophonistes…

Cette version du document a pour destinataires principaux les porteurs de projet et les acteurs de la filière industrielle. Elle doit permettre de guider la demande des porteurs de projet et de structurer l'offre de la filière.

3.4. Organisation du document

Les premiers chapitres présentent le document CARMO dans son contexte (chapitre 1), introduisent les concepts fondamentaux (chapitre 2) et décrivent l'organisation du document tout en proposant un guide de lecture (chapitre 3).

Le chapitre 4 positionne le document CARMO vis-à-vis des référentiels connexes.

Une vue d'ensemble est ensuite (chapitre 5) proposée sous deux angles, dans un premier temps celui de l'usage, puis dans un deuxième temps celui d'une architecture de référence.

Les grandes fonctions et concepts à connaitre sont décrits dans les chapitres 6 à 9.

Un ensemble de recommandations liées à l'acquisition des équipements mobiles et des outils de gestion associés est ensuite adressé aux acteurs concernés dans les chapitres 10 à 19, qui identifient les principaux critères de choix ainsi que les prérequis d'infrastructure et des outils de gestion. Un récapitulatif de toutes les recommandations, et des seules recommandations (avec mise en exergue des exigences), est fourni en annexe du présent document afin d'en présenter une vision globale.

Enfin, les chapitres 20 à 22 décrivent les bonnes pratiques liées à l'organisation d'un projet mobilité dans l'éducation.

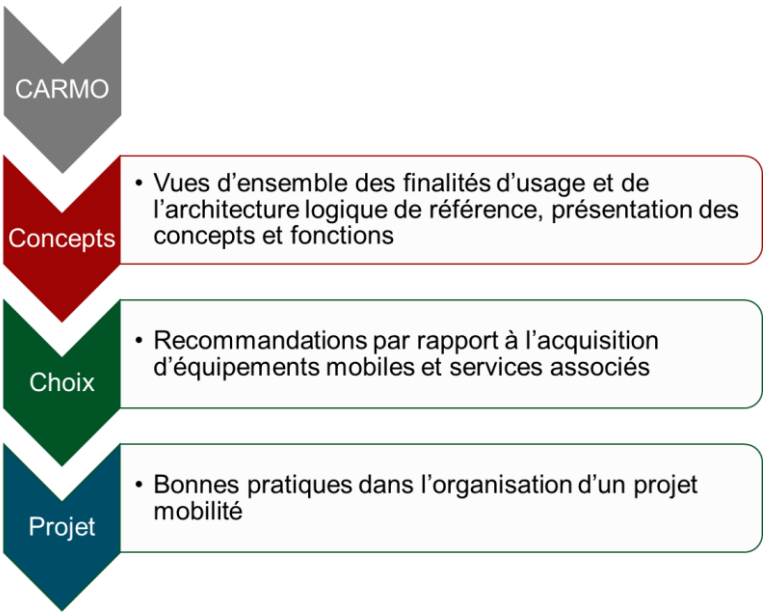


Illustration 1 : Organisation du document

Un glossaire figurant en annexe donne les définitions de certains termes, présentés en italique la première fois qu'ils sont cités dans le document.

3.5. Guide de lecture

Ce paragraphe propose, à titre indicatif, une sélection de chapitres recommandés selon la préoccupation particulière du lecteur.

3.5.1. Compréhension générale

Pour obtenir une vue d'ensemble des services et fonctions abordés, des informations sur les termes utilisés dans le domaine de la mobilité et les notions qui s'y rattachent, les lectures recommandées sont :

- chapitre 5 « Accès à une ressource numérique depuis un équipement mobile : vues d'ensemble » ;
- chapitre 6 « Présentation des fonctions : introduction » ;
- chapitre 7 « Présentation des fonctions : l'équipement mobile» ;
- chapitre 8 « Présentation des fonctions : ressource numérique » ;
- chapitre 9 « Présentation des fonctions : utilisateurs et accès aux ressources ».

Ces préoccupations peuvent intéresser tous les acteurs.

3.5.2. Choisir un équipement

Pour obtenir des éléments d'appréciation dans le choix d'un équipement mobile, notamment les fonctionnalités attendues de l'équipement mobile, le support et les étapes de préparation, les lectures recommandées sont :

- chapitre 11 « Critères de choix d'un mobile » ;
- annexe B « Exemple de grille de choix d'un équipement mobile ».

Pour le cas particulier des dispositifs de type « classe mobile », voir le chapitre 19 « Classes mobiles ».

Ces préoccupations peuvent intéresser les porteurs de projets et potentiellement les acteurs de la filière industrielle.

3.5.3. Choisir les outils associés

Les offres du marché permettant le déploiement et la gestion des équipements regroupent généralement plusieurs fonctions : gestion de flotte, distribution des applications mobiles, gestion de contenu (communément appelées respectivement MDM, MAM, MCM[2]). Dans le présent document, on utilisera parfois l'appellation générique « MxM » pour désigner indifféremment l'une ou l'autre de ces fonctions.

Pour obtenir des éléments d'appréciation pour la commande de ces outils, les lectures recommandées sont :

- fonction de gestion de flotte : chapitre 12 « Gestion des équipements mobiles (communément appelée MDM) » ;
- fonction de distribution des applications mobiles : chapitre 13 « Distribution des applications mobiles (communément appelée MAM) » ;
- fonction de gestion de contenu : chapitre 16 « Gestion des productions numériques (communément appelée MCM) ».

[2] Mobile Device Management, Mobile Application Management, Mobile Content Management : voir glossaire

En complément, afin de mettre en œuvre les pratiques pédagogiques et les projets éducatifs, des fonctions de « gestion de classe » sont nécessaires. Voir au chapitre 17 « Services fonctionnels de gestion de classe ».

Ces préoccupations peuvent intéresser les porteurs de projets et potentiellement les acteurs de la filière industrielle.

3.5.4. Gérer un projet mobilité

Pour s'assurer des éléments importants à prendre en compte dans une démarche de lancement d'un projet de mise en œuvre d'équipements mobiles et de ressources associées, les lectures recommandées sont :

- chapitre 18 « Support logiciel » ;
- chapitre 20 « Observation des usages » ;
- chapitre 21 « Gestion d'un projet mobilité » ;
- chapitre 22 « Conduite du changement ».

Ces préoccupations s'adressent principalement aux porteurs de projet.

3.5.5. Proposer des ressources

Pour les préoccupations sur les types de ressources à déployer sur les équipements mobiles et contraintes associées, les lectures recommandées sont :

- chapitre 8 « Présentation des fonctions : ressource numérique » ;
- chapitre 14.4 « Authentification ».

3.5.6. Sécurité

Les préoccupations de sécurité, transverses à tous les domaines, ont été regroupées dans un chapitre spécifique : le chapitre 14 « Sécurité ».

3.5.7. Grille récapitulative des recommandations

Une grille récapitulative des recommandations figure à l'annexe C.

4. Référentiels connexes et guides

Le cadre de référence CARMO n'est pas un document isolé, il s'appuie sur d'autres référentiels et guides qui précisent le contexte dans leur domaine respectif, notamment le cadre de référence CARINE et le SDET qui s'inscrivent dans le plan d'ensemble que constitue le S3IT (schéma stratégique des systèmes d'information et des télécommunications).

4.1. Référentiel Wi-Fi

La finalité de ce référentiel est d'aider à la conception et à la mise en œuvre d'une infrastructure Wi-Fi répondant aux besoins de l'établissement scolaire ou de l'école. Il s'adresse en priorité aux chefs d'établissement et directeurs d'école, aux directions des systèmes d'information académiques et aux collectivités territoriales.

Il vise à apporter aux différents acteurs concernés les éléments pédagogiques, juridiques et techniques à prendre en compte lors de la mise en place du Wi-Fi en établissement ou en école, afin de les aider à obtenir une infrastructure fiable et adaptée aux besoins.

Il comprend une présentation des contextes et cas d'usage pouvant conduire à recourir au Wi-Fi dans les établissements scolaires et les écoles, des éléments juridiques et des recommandations techniques de mise en œuvre.

Le référentiel Wi-Fi est disponible en ligne sur le site éduscol[3].

4.2. S2I2E – CARINE (Cadre de Référence des services d'Infrastructures Numériques d'Établissements scolaires et d'écoles)

Le référentiel CARINE (CAdre de Référence des services d'Infrastructures Numériques d'Établissements scolaires et d'écoles) a pour objet de fournir un cadre de référence permettant à l'éducation nationale et aux collectivités territoriales d'organiser en commun les réseaux et services numériques des établissements scolaires et des écoles.

Ce référentiel est issu de la refonte du CRS2i2e (Cadre de Référence des Services intranet / internet d'établissements scolaires et d'écoles) qu'il remplace.

Le référentiel CARINE est disponible en ligne sur le site éduscol[4].

4.3. SDET (Schéma directeur des espaces numériques de travail)

Pour définir les services attendus dans les espaces numériques de travail et pour formaliser les préconisations organisationnelles, fonctionnelles et techniques, le ministère publie le SDET (Schéma Directeur des Espaces numériques de Travail).

Le SDET est disponible en ligne sur le site éduscol[5].

[3] http://eduscol.education.fr/cid89186/referentiel-wi-fi.html
[4] http://eduscol.education.fr/CARINE
[5] http://eduscol.education.fr/SDET

4.4. Référentiels ANSSI (Agence nationale de la sécurité des systèmes d'information)

4.4.1. Recommandations de sécurité relatives aux mobiles multifonction

Ce document a pour objectif de sensibiliser le lecteur aux principaux risques de sécurité des terminaux mobiles et d'indiquer des recommandations de sécurité génériques à appliquer pour les limiter.

Ce recueil de bonnes pratiques est disponible en ligne sur le site de l'ANSSI[6].

La pertinence de ces recommandations est à évaluer en fonction du contexte et leur application sera fonction des enjeux et des objectifs de sécurité.

4.4.2. Recommandations de sécurité relatives aux réseaux Wi-Fi

L'objet de ce document est de guider le lecteur dans le choix des meilleurs paramètres pour la bonne sécurisation d'un réseau Wi-Fi. Le particulier non averti y trouvera des recommandations simples à appliquer pour la mise en place d'un réseau Wi-Fi personnel, tandis que l'administrateur réseau en entreprise y trouvera des informations et recommandations complémentaires applicables à un système d'information.

Ce recueil de bonnes pratiques pour sécuriser les accès Wi-Fi est disponible en ligne sur le site de l'ANSSI[7].

La pertinence de ces recommandations est à évaluer en fonction du contexte et leur application sera fonction des enjeux et des objectifs de sécurité.

4.4.3. RGS (Référentiel général de sécurité)

Le référentiel général de sécurité (RGS) est un référentiel destiné à sécuriser les échanges électroniques de la sphère publique. Pour une autorité administrative, appliquer le RGS permet de garantir aux citoyens et autres administrations que le niveau de sécurité de ses systèmes d'information est bien adapté aux enjeux et aux risques et qu'il est harmonisé avec ceux de ses partenaires.

Les documents constitutifs du RGS sont disponibles en ligne[8].

4.5. RGAA (Référentiel général d'accessibilité pour les administrations)

L'article 47 de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées fait de l'accessibilité une exigence pour tous les services de communication publique en ligne de l'État, les collectivités territoriales et les établissements publics qui en dépendent. Il stipule que les informations diffusées par ces services doivent être accessibles à tous.

[6] http://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-aux-ordiphones
[7] http://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-aux-reseaux-wifi
[8] https://references.modernisation.gouv.fr/securite

Le décret n°2009-546 du 14 mai 2009 (pris en application de l'article 47 de la loi n° 2005-102 du 11 février 2005 sur l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées) impose une mise en œuvre de l'accessibilité dans un délai de deux ans (à partir de la publication du décret) pour les services de communication publique en ligne de l'État et des établissements publics qui en dépendent, et de trois ans pour les services de communication publique en ligne des collectivités territoriales et des établissements publics qui en dépendent.

Le Référentiel général d'accessibilité pour les administrations (RGAA), à forte dimension technique, offre une traduction opérationnelle des critères d'accessibilité issus des règles internationales ainsi qu'une méthodologie pour vérifier la conformité à ces critères.

Le RGAA, dont la version 3.0 a été officialisée par arrêté ministériel le 29 avril 2015, est disponible en ligne[9].

4.5.1. A2RNE (Adaptabilité et accessibilité des ressources numériques pour l'École)

Pour accompagner la scolarisation des élèves en situation de handicap, le ministère mène une politique de soutien à la production et au développement des usages de ressources pédagogiques numériques adaptées. Le numérique permet en effet d'offrir des réponses pertinentes aux besoins des élèves en situation de handicap : leurs contenus peuvent, via des traitements informatiques appropriés, être aisément adaptés pour répondre aux besoins spécifiques des publics concernés. De fait, les ressources numériques pour l'École se doivent d'exploiter ces opportunités ; d'autant qu'au-delà de l'aspect éthique, l'expérience montre aussi que les efforts réalisés pour prendre en compte les besoins éducatifs particuliers des élèves en situation de handicap sont bénéfiques à tous les élèves de la classe.

À cet effet, le ministère a publié des guides de bonnes pratiques à destination des auteurs de ressources numériques pour l'école et des industriels de la filière, pour la conception et la production de ressources numériques accessibles et adaptables pour et par les personnes en situation de handicap.

Ces propositions de bonnes pratiques pour l'accessibilité et l'adaptabilité des ressources numériques pour l'École (A2RNE) sont disponibles en ligne sur le site éduscol[10].

4.6. RGI (Référentiel général d'interopérabilité)

Le RGI est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration. Ces recommandations constituent les exigences pour favoriser l'interopérabilité. Elles permettent aux acteurs cherchant à interagir et donc à favoriser l'interopérabilité de leur système d'information, d'aller au-delà de simples arrangements bilatéraux.

Une version 2 de ce référentiel a été publiée en avril 2016.

Le RGI est disponible en ligne[11].

4.7. Guide des projets pédagogiques s'appuyant sur le BYOD / AVEC

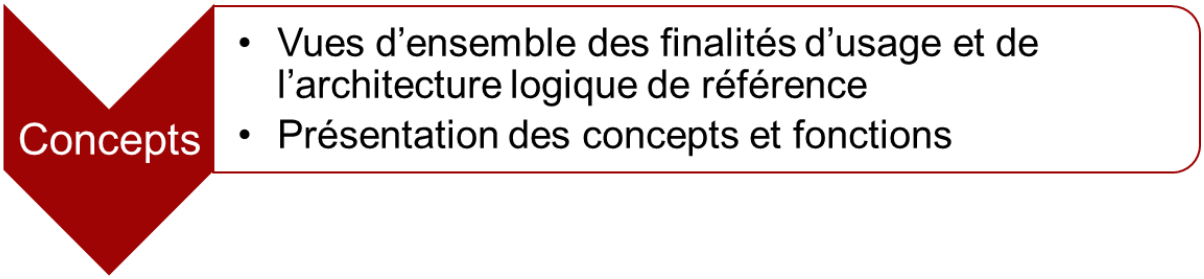
Ce document constitue un guide des projets BYOD. À ce titre, il vise à être un point d'entrée pratique et opérationnel pour les porteurs de projets pédagogiques s'appuyant sur le BYOD.

[9] https://references.modernisation.gouv.fr/rgaa-accessibilite
[10] http://eduscol.education.fr/A2RNE
[11] https://references.modernisation.gouv.fr/interoperabilite

Il regroupe ainsi un ensemble de conseils, recommandations et bonnes pratiques pour élaborer et mettre en place un projet BYOD. En cela, il fournit une approche pragmatique sur les différentes problématiques spécifiques aux projets BYOD en traitant des aspects techniques, organisationnels juridiques et pédagogiques. Cependant, ce guide ne constitue pas un schéma directeur pour la réalisation de cahiers des charges.

Le guide est disponible en ligne[12].

[12] https://eduscol.education.fr/cid128686/guide-des-projets-pedagogiques-s-appuyant-sur-le-byod-avec.html


Concepts
• Vues d'ensemble des finalités d'usage et de l'architecture logique de référence
• Présentation des concepts et fonctions

5. Accès à une ressource numérique depuis un équipement mobile : vues d'ensemble

Ce chapitre s'adresse à tous les acteurs des projets d'équipements mobiles.

Il fournit une vue d'ensemble des enjeux des projets d'équipements mobiles, avec deux angles de vue :

- la vue « métier » s'intéresse aux questions suivantes : quels services sont attendus d'un équipement mobile dans l'éducation, et quels sont ses apports aux pratiques et missions éducatives ?
- la vue architecture de référence indique quelles sont les fonctions (matérielles, logicielles et de prise en compte de l'utilisateur) qui vont permettre de rendre les services attendus par les usagers dans l'écosystème.

Les cas d'usage décrits s'inscrivent dans le respect des différentes dispositions légales et règlementaires en vigueur applicables aux projets d'équipements mobiles, en particulier des principes de sécurité, d'intégrité et de confidentialité des données à caractère personnel (règlementation en matière de protection des données à caractère personnel, de propriété intellectuelle…).

5.1. Vue d'ensemble des services pour les usagers

L'équipement mobile peut contribuer à rendre des services de plusieurs natures, pour mettre le numérique au service des apprentissages et du socle commun de connaissances, de compétences et de culture.

Les services rendus depuis un équipement mobile à l'usager sont présentés dans ce chapitre sans préjuger de l'architecture applicative permettant de fournir ces services (applications natives, en ligne, ENT/hors ENT…).

Ces services ont été définis au cours d'une étude d'expression de besoins, impliquant les principaux acteurs concernés.

Pour les élèves, l'équipement mobile doit contribuer à 7 services principaux :

- accéder à des ressources numériques (contenus et services) de qualité pour les apprentissages ;
- développer l'autonomie, la création et la créativité de l'élève ;
- renforcer la relation école-famille et le suivi de l'activité scolaire ;
- assurer la continuité pédagogique ;
- permettre le travail en équipe, la mutualisation ;
- promouvoir la mobilité dans l'usage de l'équipement mobile et des applications de l'ENT ;
- développer la maîtrise des outils numériques et la construction d'une culture numérique.

Pour les enseignants, l'équipement mobile doit contribuer à 5 services principaux :

- mettre en œuvre les pratiques pédagogiques ;
- personnaliser les parcours et les apprentissages ;
- permettre le travail en équipe, la mutualisation ;
- promouvoir la mobilité dans l'usage de l'équipement mobile et des applications de l'ENT ;
- développer la maîtrise des outils numériques et la construction d'une culture numérique.

Remarque : les 3 derniers services sont communs aux élèves et aux enseignants.

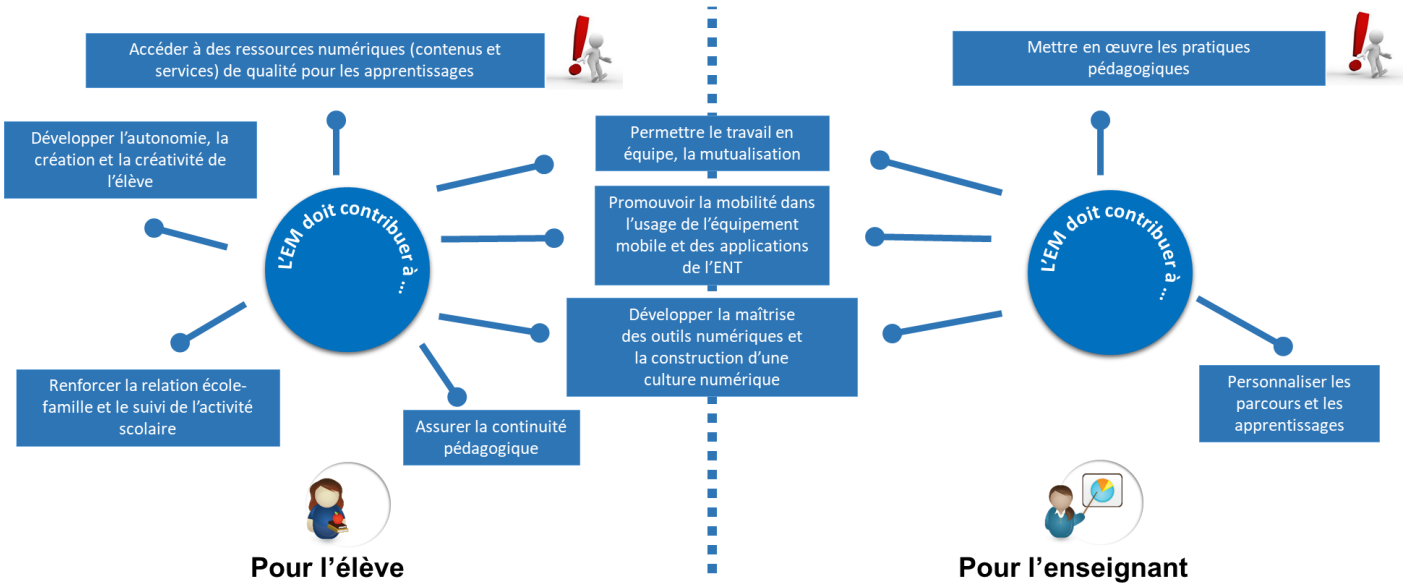


Illustration 2 : Vue d'ensemble des services pour les usagers

Pour chacun de ces services, un tableau d'exemples de cas d'usages et d'apports de l'équipement mobile est proposé. L'ensemble de ces services doit être déployé dans le respect des dispositions applicables en matière de protection des données en particulier le RGPD et la loi informatique, fichiers et libertés modifiée en 2018.

5.1.1. Accéder à des ressources numériques (contenus et services) de qualité pour les apprentissages

Exemples de cas d'usage :

- l'enseignant repère des ressources pédagogiques pertinentes, les commande par le biais de son établissement et les met à disposition de ses élèves ;
- l'enseignant produit des ressources pédagogiques et les met à disposition de ses élèves ;
- un travail réalisé par un élève est soumis à la critique ou à la validation des autres : un exercice / une démarche / une scène est filmé(e) pour une autocorrection en petit groupe ou de manière collective ;
- les élèves accèdent aux ressources mises à disposition par le centre de documentation de leur établissement ;
- des exercices favorisant le travail collectif à l'aide de supports mobiles sont proposés aux élèves ;
- les travaux individuels et collectifs sont effectués en alternance ;
- des projets d'apprentissage transdisciplinaires sont proposés ;
- des ressources « pour aller plus loin » sont proposées à l'élève sur les sujets qui l'intéressent ou qu'il ne maitrise pas.

Apports de l'équipement mobile :

- l'équipement mobile apporte des Outils multimédia intégrés pour produire du contenu d'une manière rapide ;

- l'équipement mobile suit l'élève dans et hors établissement ce qui permet d'accéder aux ressources toujours de la même manière ;

- l'équipement mobile individualise le support mais permet d'accéder à des outils et espaces de travail communs ;

- l'équipement mobile couplé à des applications dédiées permet un changement rapide et facile de configuration de la classe ;

- l'équipement mobile et la ressource numérique facilitent l'utilisation de dispositifs de compensation pour les élèves en situation de handicap.

5.1.2. Mettre en œuvre les pratiques pédagogiques

Exemples de cas d'usage :

- lancer une application sur tous les équipements mobiles de la classe et bloquer les équipements mobiles sur cette application (de type mode single App) ;
- restreindre ou autoriser l'accès à certaines fonctionnalités/applications de l'équipement mobile ;
- construire ses cours pour un usage à partir de l'équipement mobile ;
- communiquer avec ses élèves (informer les élèves d'un changement de classe, partager son écran en classe pour aider l'élève…) ;
- communiquer avec ses collègues ;
- connecter l'équipement mobile à un dispositif de projection afin de donner un support visuel à son cours, projeter l'écran d'un ou plusieurs équipements mobiles sur l'équipement de visualisation collective ;
- remplir les bulletins ;
- réserver les ressources (salles, matériels…) ;
- corriger des devoirs produits de manière numérique ;
- accéder aux autres services de l'ENT (exemple : donner les devoirs) ;
- enrichir la palette d'outils au service des enseignants ;
- former des enseignants ;
- personnaliser l'environnement de travail aux besoins spécifiques de son utilisateur (activité individualisée, situation de handicap…) ;
- accéder rapidement aux contenus mobilisables pour une séquence pédagogique (documents de travail, productions personnelles, traces mémoire…).

Apports de l'équipement mobile :

- focaliser l'attention de l'élève dans les séquences pédagogiques ;
- modifier dynamiquement la configuration de l'équipement mobile ;
- permettre la diffusion rapide de contenu ;

- accéder de manière sécurisée à des moyens de communication indépendamment du lieu et du moment ;
- accéder de manière sécurisée à distance à l'information.

5.1.3. Contribuer à renforcer la relation école-famille et le suivi de l'activité scolaire

Exemples de cas d'usage :

- rendre accessible en tous lieux et à tout moment les services de l'ENT :
  - emplois du temps, cahier de textes, consignes de travail,
  - services de vie scolaire,
  - vie de l'établissement (menus de la cantine, agenda des activités…),
  - collaboration (élèves entre eux, entre élèves et enseignants),
  - communication (entre famille et établissement),

- informations (ex. : transports) ;

- permettre aux parents de suivre les travaux numériques effectués en classe.

Apports de l'équipement mobile :

- répondre aux difficultés d'accès à l'équipement dans certaines familles ;
- permettre la consultation des travaux numériques hors de l'établissement ;
- permettre la consultation des travaux et des ressources numériques et favoriser la communication famille/établissement pour les parents, élèves ou enseignants en situation de handicap.

5.1.4. Développer la maitrise des outils numériques et la construction d'une culture numérique

Exemples de cas d'usage :

- éduquer les élèves et les enseignants aux médias numériques (sensibilisation à la sécurité et à la protection des données, droit des mineurs, droit à l'image, propriété intellectuelle) ;
- généraliser le développement du numérique éducatif ;
- responsabiliser l'élève face au numérique : législation, éducation aux médias et à l'information, usage responsable des ressources ;
- autoriser un usage personnel responsable et complémentaire à l'activité pédagogique.

Apports de l'équipement mobile :

- utilisation possible dans n'importe quelle situation d'apprentissage ;
- facilité d'utilisation (démarrage instantané, ergonomie) ;
- équipement fourni individuellement à l'élève pour se responsabiliser dans ses propres usages.

5.1.5. Favoriser le développement de l'autonomie, la création et la créativité

Exemples de cas d'usage :

- enrichir facilement ses productions avec des fonctions multimédia embarquées, directement utilisables ;
- permettre à l'élève de s'auto évaluer et d'adapter son travail et ses exercices ;
- permettre à l'élève d'avancer à son rythme, indépendamment des autres ;
- faciliter l'autonomie pour les élèves en situation de handicap ;
- disposer immédiatement après une activité physique de statistiques détaillées ;
- annoter les cours/contenus en fonction de ses besoins ;
- préparer des documents ;
- favoriser l'observation individualisée d'œuvres ;
- permettre le travail individualisé sur des œuvres ;
- faciliter l'utilisation de baladodiffusion ;
- faciliter la lecture d'œuvres, audio, vidéo, texte…
- diffuser facilement des adresses web via un *QR Code*.

Apports de l'équipement mobile :

- capturer un son ;
- capturer une image (animée ou non) ;
- offrir des possibilités artistiques et multimédias démultipliées (exemple : composer une musique, prendre des photos, modifier des images, créer une séance filmée) ;

- filmer et revoir une action ;

- permettre l'utilisation d'appareils ou d'outils de compensation de handicap (par exemple : plage braille, scanners, capteurs de souffle, capteurs musculaires) ;

- remplacement d'appareils de mesure (exemple : voltmètre oscilloscope) à l'aide de capteurs additionnels ;
- transformation en microscope à moindres frais ;

- effectuer des recherches ;
- accès simples à des outils de natures variées, permettant de diversifier les méthodes d'évaluation.

5.1.6. Contribuer à personnaliser les parcours et les apprentissages

Exemples de cas d'usage :

- proposer aux élèves des ressources pédagogiques différenciées (exercices, cours…) selon leur niveau et leur avancement et/ou leur situation face à un handicap, avec disponibilité individuelle du terminal ;
- visionner en aval les séquences d'apprentissage afin d'identifier les points de blocage ;
- visualiser en temps réel la production de l'élève.

Apports de l'équipement mobile :

- suivre le travail que chaque élève réalise sur l'équipement mobile qu'il utilise de façon centralisée, et fournir des consignes en fonction de l'avancement ;
- capture des séquences d'apprentissage ;
- partage d'écran ;
- prise en charge des situations de handicap, adaptabilité et accessibilité des ressources numériques permettant une personnalisation adaptée.

5.1.7. Contribuer au travail en équipe et à la mutualisation

Exemples de cas d'usage :

- diffusion d'une expérience aux élèves sans avoir à déplacer tout le groupe classe ;
- mise en commun de résultats (par exemple expérience filmée) ;
- utilisation d'outils basés sur l'interaction/les interactions :
  - utiliser un dispositif (forum, flux…) pour permettre aux élèves de poser des questions (auxquelles l'enseignant et les autres élèves pourront répondre),
  - proposer un sondage / QCM en temps réel qui permet un retour immédiat sur la compréhension du cours par les élèves et les ajustements éventuellement nécessaires ;
- soumission d'un travail d'élève à la critique ou la validation des autres :
  - filmer une démarche / une scène / un exercice pour une auto correction en petit groupe ou collective.

Apports de l'équipement mobile :

- envoi simplifié de données ;
- interactivité quasi temps-réel ;
- partage et mise à disposition du contenu facilités (tableaux numériques ou équipements mobiles du groupe) ;
- ajustements éventuels immédiats sur la compréhension du cours par les élèves.

5.1.8. Contribuer à assurer la continuité pédagogique (en particulier établissement – hors établissement)

Exemples de cas d'usage :

- offrir la possibilité d'un lien entre les activités scolaires en classe et hors de l'établissement (voyages ou sorties scolaires) ;
- disposer des mêmes ressources pédagogiques utilisées en classe (manuels, cours, exercices, logiciels…) en tous lieux (domicile notamment) ;
- permettre de continuer ou reprendre à la maison les exercices numériques vus en classe ;
- accompagner les élèves en situation de handicap ;
- faciliter le rattrapage des cours manqués (maladie, absence…) ;
- permettre aux parents de consulter les productions de leurs enfants ;
- inclure des élèves scolarisés en dehors de la classe (domicile familial, centres médicaux, hôpital…) ou accompagner les élèves et enseignants à mobilité réduite.

Apports de l'équipement mobile :

- volume et poids du cartable (par rapport aux manuels papiers) ;
- synchronisation de données ;
- ressources et services accessibles à distance ;
- interactions avec la classe possibles à distance ;
- peut également fonctionner en l'absence de connexion.

5.1.9. Équipement mobile : promouvoir la mobilité dans l'usage des ENT

Exemples de cas d'usage :

- stocker des données de production de l'équipement mobile directement sur l'espace de stockage personnel de l'ENT ;
- partager un document ou une production personnelle dans l'espace de partage et de collaboration de l'ENT ;
- faire l'appel depuis un équipement mobile sur un terrain de sport, hors accès au poste de connexion d'accès à l'ENT et synchroniser les données de l'appel de manière sécurisée (code d'authentification demandé) avec le service de gestion d'absences de l'ENT ;
- procéder à des enregistrements audio, photo et vidéo et les envoyer directement dans l'espace de stockage de l'ENT ;
- informer les usagers sur les événements de l'établissement par notification poussée (push) des billets d'actualité de l'ENT ou d'évènements particuliers (par exemple, un retard sur le retour de livres à la bibliothèque).

Apports de l'équipement mobile :

- accéder à distance aux données de l'ENT ;
- disposer d'outils de production de contenus multimédia directement en mobilité (audio, photo et vidéo) ;

- disposer d'un moyen additionnel de sécurisation de l'accès aux données de la vie scolaire. Par exemple, l'accès à l'application mobile pour faire l'appel hors de l'établissement peut être sécurisée par code pin pour assurer que seul l'enseignant peut modifier les données. Sans équipement mobile, l'appel se fait souvent sur un papier qui parfois peut être confié à un élève pour être déposé par un élève dans le bureau de vie scolaire et qui pourrait, par conséquent, le modifier ;
- disposer d'un moyen de sécurisation additionnelle pour l'accès à l'ENT (par exemple, en utilisant un double facteur d'authentification grâce à l'envoi d'une notification sur l'EIM de l'utilisateur lors d'une tentative d'accès à l'ENT) ;
- dans le cas des EIM, permettre à l'utilisateur d'étendre les capacités de stockage et de partage entre ENT et EIM.

5.2. Vue d'ensemble de l'architecture de référence

Pour fournir les services métier décrits dans le paragraphe précédent, le projet d'équipements mobiles doit permettre de répondre à l'ensemble des préoccupations matérielles, logicielles et utilisateurs.

Ce paragraphe présente le schéma d'ensemble constituant la vue logique de l'architecture fonctionnelle. Il vise à présenter de façon synthétique, par une structuration et une visualisation à haut niveau, l'ensemble des thématiques à couvrir lors la mise en œuvre d'un projet d'équipements mobiles.

Ces thématiques sont les suivantes :

- gestion des cycles de vie :
  - gestion du cycle de vie des ressources numériques,
  - gestion du cycle de vie des équipements mobiles et accessoires ;
- support :
  - support matériel,
  - support logiciel ;
- services de gestion des productions numériques :
  - stockage de productions numériques,
  - sauvegarde / restauration et archivage des productions numériques,
  - synchronisation des données ;
- services fonctionnels :
  - services de communication et de collaboration,
  - services informationnels et documentaires,
  - services de production pédagogique et éducative,
  - services d'accompagnement de la vie de l'élève,
  - services de gestion de classe ;
- services socles des équipements mobiles :
  - notification,
  - stockage local,
  - services d'accès réseau et connectivité,
  - gestion de contacts,
  - système d'exploitation,
  - repérage spatio-temporel,
  - capture multimédia,
  - gestion des environnements ;
- gestion des équipements mobiles :

- gestion de l'inventaire des équipements mobiles et des accessoires,
- monitorage / compte rendu / statistiques des équipements mobiles,
- application des politiques de sécurité,
- sauvegarde et restauration des équipements mobiles,
- configuration des équipements mobiles,
- application de la mise à jour des systèmes d'exploitation,
- gestion des profils utilisateur ;

- distribution des applications mobiles :
  - gestion de l'inventaire des applications mobiles,
  - association ressource / profil équipement mobile et / ou profil utilisateur,
  - monitorage / compte rendu / statistiques des applications distribuées,
  - store / portail d'accès aux ressources ;
- service d'infrastructure pour l'établissement :
  - gestion des systèmes informatiques (infogérance serveurs) et composants réseaux,
  - services réseau,
  - monitorage / compte rendu / statistiques de l'infrastructure ;
- services de sécurité :
  - authentification,
  - autorisation,
  - détection du non-respect des politiques de sécurité,
  - propagation des identités,
  - gestion des annuaires,
  - définition des politiques de sécurité.

Le schéma présenté en Illustration 20 reprend ces mêmes informations sous forme graphique.

Remarque : ces grands blocs de fonctions se retrouvent dans les chapitres suivants (chapitres 1 à 9) qui explicitent, dans une vision large et sans restriction, les possibilités offertes par un équipement mobile et l'écosystème qui lui est lié : la gestion, les ressources, la sécurité.

Remarque : cette architecture de référence est une représentation conceptuelle et structurée des services susceptibles d'être mis en œuvre dans des projets d'équipements mobiles. Selon le type de projet (EIM, classe mobile et/ou BYOD), les services ou fonctions pourront être plus ou moins pertinents. Les différents chapitres consacrés aux recommandations fournissent des précisions permettant d'identifier les services et fonctions les plus adaptés à chaque type de projet.

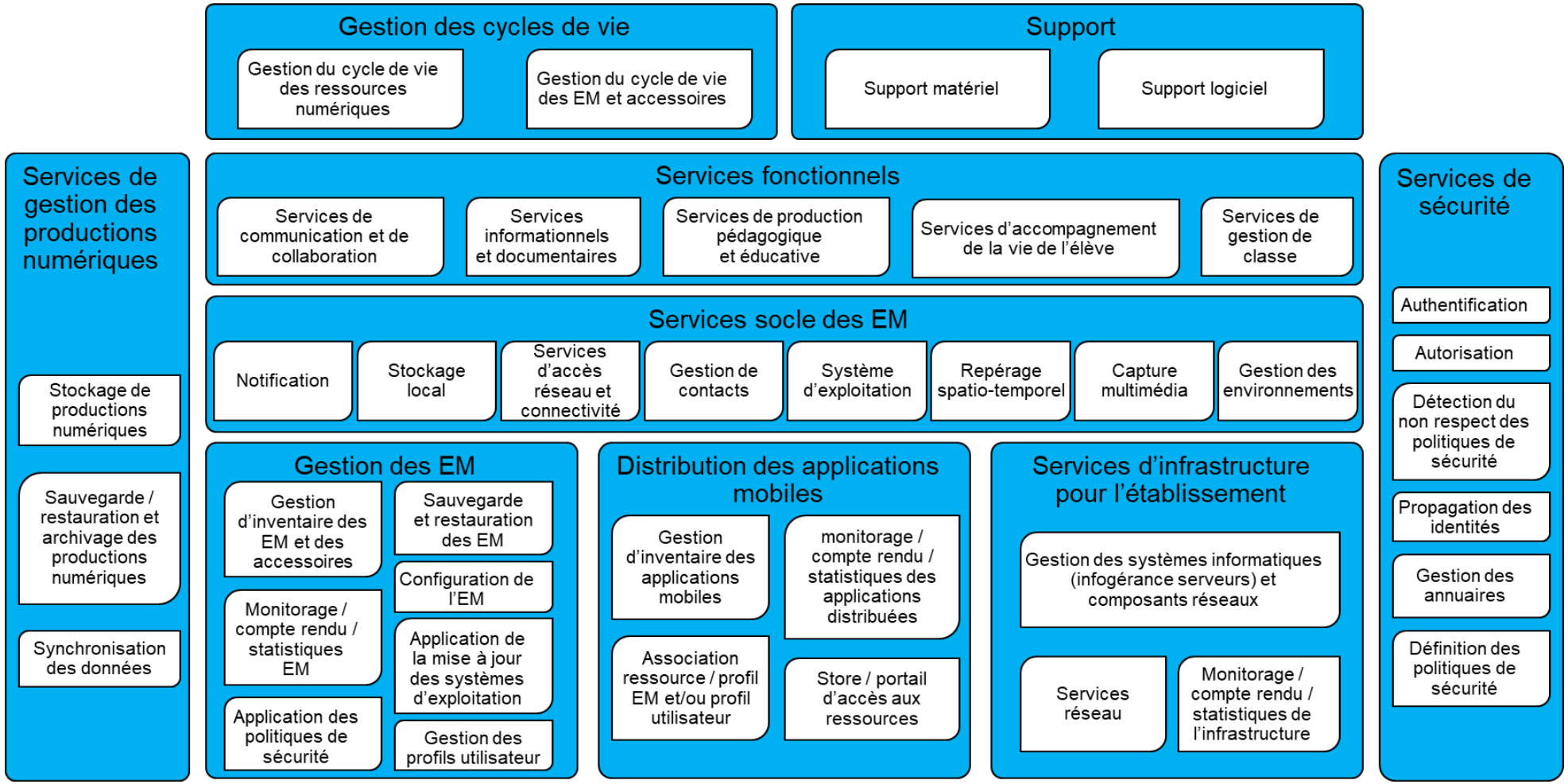


Illustration 3 : Vue d'ensemble de l'architecture de référence

6. Présentation des fonctions : introduction

Les fonctions portées par l'architecture de référence peuvent être analysées autour d'un triptyque :

- l'équipement mobile, qui porte les préoccupations matérielles à savoir :
  - le matériel lui-même, avec ses caractéristiques et la sécurité associée,
  - l'outil qui va permettre de gérer le parc d'équipements mobiles,
  - la gestion dans le temps de l'équipement mobile et son support ;
- la ressource, qui porte les préoccupations logicielles :
  - les différents types de ressources fonctionnelles et techniques,
  - l'outil qui va permettre de gérer le déploiement des applications sur les équipements mobiles,
  - le support de la ressource,
  - la gestion dans le temps, de l'acquisition jusqu'à un arrêt de l'abonnement ;
- l'utilisateur qui va utiliser des ressources sur l'équipement mobile et va donc devoir être authentifié et gérer ses productions numériques.

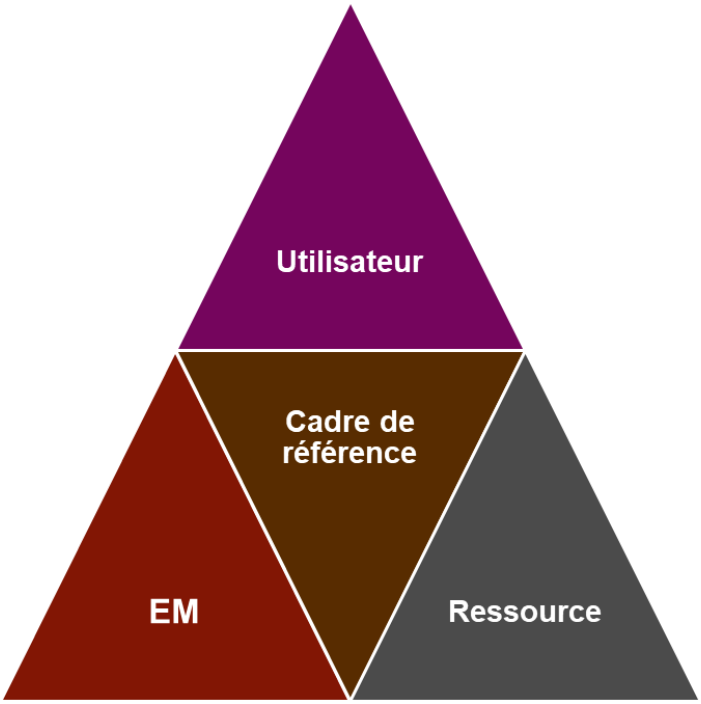


Illustration 4 : Triptyque Équipement mobile / Ressource / Utilisateur

7. Présentation des fonctions : l'équipement mobile

7.1. Caractéristiques et fonctionnalités d'un équipement mobile

Indépendamment des implémentations spécifiques de chaque fabricant d'équipements mobiles, il existe un ensemble de caractéristiques communes aux équipements mobiles.

7.1.1. Système d'exploitation

Un système d'exploitation est un ensemble de programmes qui dirige l'utilisation des capacités d'un équipement mobile par des logiciels applicatifs. Les grandes catégories de capacités sont :

- les capacités de stockage sur des mémoires et des disques durs ;
- les capacités de calcul du (ou des) processeur(s) ;
- les capacités de communication vers des périphériques (clavier, casque audio, espace de stockage externe…) ou via le réseau (Wi-Fi ou cellulaire lorsqu'applicable).

Les principaux systèmes d'exploitation des équipements mobiles du marché actuel (décembre 2018) sont :

Système d'exploitation	Éditeur
Android	Google
Chrome OS	Google
iOS	Apple
Windows	Microsoft

Tableau 1 : Principaux systèmes d'exploitation des équipements mobiles

Les OS proposent des dispositifs d'accessibilité au sens du handicap, ce qui permet d'aider les personnes atteintes d'incapacités physiques ou cognitives, de troubles et de déficiences. Ces aides techniques couvrent plusieurs fonctions comme : l'agrandissement des caractères (fonction loupe), la vocalisation des caractères à partir de lecteurs d'écrans, la conversion des caractères en braille, l'affichage d'alertes visuelles pour les malentendants… Les solutions d'assistance sont soit des applications intégrées au système d'exploitation dites « natives » soit des extensions téléchargeables. Quel que soit le dispositif retenu, celui-ci ne doit pas conduire à collecter des catégories particulières de données au sens du RGPD et notamment des données de santé.

7.1.2. Notification

Les notifications sont des messages spécifiques associés à une application installée sur l'équipement mobile. L'activation de la réception et du traitement des notifications pour une application donnée nécessite un accord de l'utilisateur lors de l'installation de celle-ci sur l'équipement mobile lorsqu'il s'agit d'un EIM.

Il existe deux formes de notification : les notifications « **locales** » générées en interne par l'application (par exemple un rappel pour une application de type agenda) et les notifications « **distantes** » émises depuis un serveur applicatif.

Dans le cas des notifications distantes, le service de notification de l'équipement mobile permet la réception de messages émis depuis une passerelle informatique (au même titre que le Short Message Service – « *SMS* » ou le Multimedia Messaging Service – « *MMS* ») et l'affichage de ces messages sur l'équipement mobile.

Une notification distante peut être personnalisée et adaptée au contexte de l'utilisateur.

Le principe de fonctionnement pour les notifications distantes est le suivant :

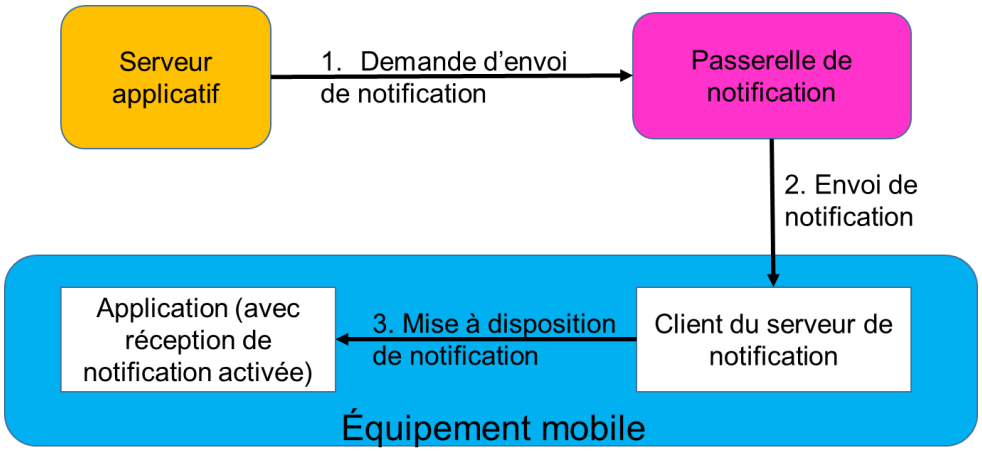


Illustration 5 : Principe de fonctionnement des notifications

1. Le serveur applicatif (associé à l'application installée sur l'équipement mobile) effectue une demande d'envoi de notification via la passerelle de notification associée au système d'exploitation de l'équipement mobile cible.
2. La passerelle envoie la notification vers l'équipement mobile via le client du service de notification présent dans le système d'exploitation de l'équipement mobile.
3. La notification est mise à disposition de l'application cible pour prise en compte et affichage (via une alerte ou un bandeau sur l'équipement mobile ou un « badge » sur l'icône de l'application) ou alerte sonore.

Pour le *SMS* et le *MMS*, les passerelles d'envoi de message sont gérées par les opérateurs télécom. Dans le cas des équipements mobiles, le service de notification est spécifique au système d'exploitation associé à l'équipement mobile ; les passerelles d'envoi de notification sont gérées par les éditeurs de ces différents systèmes d'exploitation des équipements mobiles. On peut à ce jour citer les principaux services suivants :

Passerelle de notification	Éditeur/ système d'exploitation
Google Cloud Messaging (GCM)[13]	Google / Android
Apple Push Notification Service (APN)[14]	Apple / iOS
Windows Push Notification Services (WNS)[15]	Microsoft / Windows

Tableau 2 : Principaux services de passerelle de notification

L'utilisation des passerelles d'envoi de notification est gratuite. La qualité de service (délai de réception de la notification, durée de vie de la notification) est spécifique à chaque passerelle et définie par l'opérateur de la passerelle. La remise des notifications n'est pas garantie.

[13] https://developer.android.com/google/gcm/gcm.html
[14] https://developer.apple.com/library/ios/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/Chapters/ApplePushService.html
[15] http://msdn.microsoft.com/en-us/library/windows/apps/hh913756.aspx

En revanche, la gestion des notifications (en particulier leur composition, l'identification des EIM cibles et la mise au format de la passerelle d'envoi) nécessite la mise en place d'une infrastructure informatique ou l'usage d'un service (au sens « Software As A Service – SaaS » du terme) lié à l'application utilisant ces notifications.

Des recommandations relatives aux risques liés aux notifications sont proposées dans le chapitre Gestion des équipements mobiles.

7.1.3. Stockage local

Les équipements mobiles comportent des dispositifs matériels internes spécifiques pour stocker les ressources suivantes :

- le micrologiciel qui s'exécute avant le démarrage du système d'exploitation ;
- le système d'exploitation ;
- le code d'exécution des applications installées sur l'équipement mobile ;
- les données associées aux applications (paramètres, traces, cache, données de contexte de l'utilisateur) ;
- les ressources numériques produites par l'utilisateur au moyen des applications disponibles sur l'équipement mobile ;
- les ressources numériques téléchargées depuis un serveur distant.

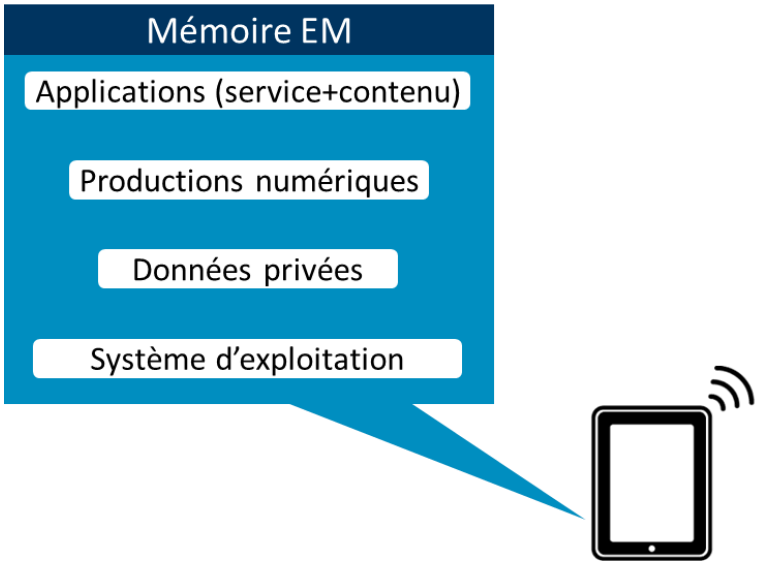


Illustration 6 : Stockage local sur l'équipement mobile

Certains systèmes d'exploitation ou matériels permettent une extension par des dispositifs externes comme une carte *microSD* (ou Micro Secure Digital Card) au moyen d'un lecteur interne intégré dans l'équipement mobile, ou comme un disque dur externe via une connectique filaire ou sans fil.

Les capacités et la sécurité des espaces de stockage sont des éléments importants à prendre en compte lors du choix d'un équipement mobile en fonction des usages visés.

7.1.4. Services d'accès réseau et connectivité

Les services de communication sans fil sont une des capacités clé des équipements mobiles ayant pour vocation à être utilisés en mobilité / nomadisme.

Ainsi, l'ensemble des équipements mobiles du marché intègre une capacité de connexion aux réseaux sans fil selon la norme Wi-Fi 802.11 (normes standards Wi-Fi).

Ceci implique que l'utilisateur puisse se connecter à un réseau Wi-Fi auquel l'équipement mobile peut accéder avec le niveau de sécurité minimal requis par le fournisseur du réseau Wi-Fi.

L'équipement mobile peut intégrer d'autres systèmes de connectivité soit pour accéder à Internet soit pour permettre une connexion directe avec d'autres matériels. L'accès à internet peut ainsi s'effectuer via un service de connexion cellulaire (réseaux télécom 3G/4G) pour autant qu'un abonnement de type « data » ait été souscrit et associé à l'équipement mobile concerné ; l'association se fait comme pour un téléphone mobile au moyen d'une carte SIM.

La connexion directe avec d'autres matériels (par exemple un autre équipement mobile, un tableau numérique) peut se faire au moyen d'autres standards de communication comme :

- le Bluetooth ;
- la communication en champ proche ou *NFC ;*
- la radio-identification ou *RFID ;*
- la projection sans fil (Miracast, WiDi, AirPlay, ChromeCast…).

Comme la connectivité Wi-Fi, le Bluetooth est un service de communication disponible sur l'ensemble des équipements mobiles du marché actuel. La liste de standards ci-dessus n'est pas exhaustive car de nouveaux services, tels le Bluetooth Low Energy, émergent progressivement. Cependant, tous les équipements mobiles ne fournissent pas nécessairement ces nouveaux services.

Au-delà des services de connectivité sans fil, les fabricants équipent les équipements mobiles de différents connecteurs physiques (au-delà du connecteur de rechargement électrique de la batterie interne) tels qu'USB, VGA, RJ45 ou HDMI. Les équipements mobiles proposent quasiment tous des prises audio (de type jack).

La liste ci-dessus n'est ni exhaustive ni généralisée à l'ensemble des équipements mobiles du marché. Les capacités de connectivité d'un équipement mobile constituent un critère de choix à prendre en compte lors de la sélection d'un matériel et à croiser avec les usages attendus. Des connecteurs permettent par exemple d'associer à l'équipement mobile des dispositifs utilisés par les élèves en situation de handicap.

Il faut également être attentif à la nature des connecteurs physiques du terminal qui peuvent être standards ou propriétaires ; dans ce dernier cas, il est nécessaire de veiller à la cohérence des équipements périphériques et des câbles de connexion associés. Les capacités de connectivité ainsi que les connecteurs physiques du terminal doivent être choisis pour assurer un niveau satisfaisant de sécurité.

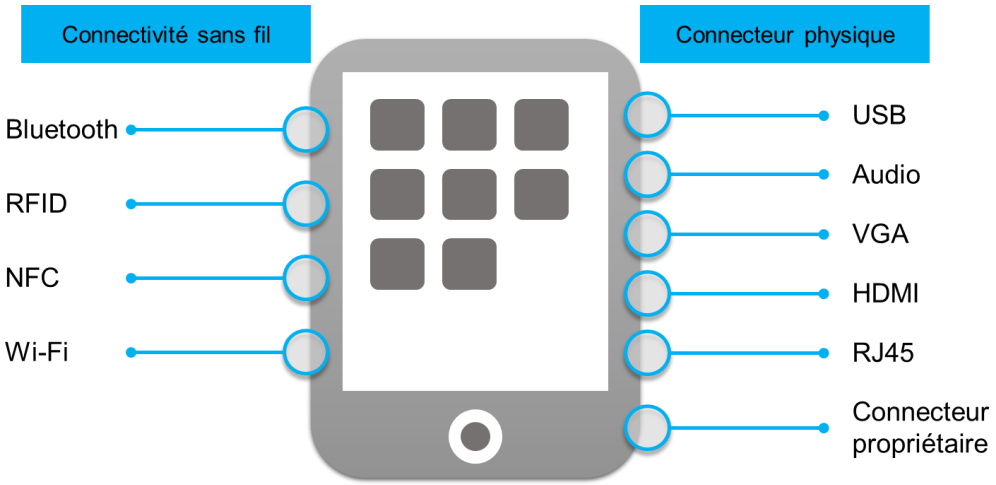


Illustration 7 : Services d'accès réseau et connectivité

7.1.5. Gestion de contacts

Les systèmes d'exploitation iOS, Android et Windows intègrent nativement une application de gestion de contacts qui permet un usage combiné avec les applications de gestion de mail et d'agenda.

Un contact est un individu identifié au moyen d'une adresse email ou d'un numéro de téléphone, qui peut être ajouté manuellement à la liste de contacts de l'utilisateur de l'équipement mobile lorsqu'il s'agit d'un EIM, ou bien via un outil de recherche (par exemple recherche intégrée dans l'application de messagerie ou bien application autonome de recherche) dans un annuaire d'utilisateurs accessible par l'outil de recherche.

Les informations contenues dans la liste des contacts peuvent ensuite (si l'utilisateur de l'EIM l'accepte) être utilisées par des applications tierces, par exemple pour déclencher un appel téléphonique, l'envoi d'un *SMS* ou pour l'usage de l'adresse du contact afin de calculer un itinéraire.

Les contacts peuvent être manuellement importés ou exportés vers ou depuis un EIM.

7.1.6. Repérage spatio-temporel

Les équipements mobiles offrent de manière générale des services permettant en continu de positionner l'équipement mobile : « à un instant donné, l'équipement mobile a telles coordonnées géographiques, a telle orientation dans l'espace et subit un mouvement de telle nature ». Ces services sont accessibles via le système d'exploitation de l'équipement mobile. Nous pouvons citer les services suivants :

- la boussole permet d'indiquer une direction ;
- l'accéléromètre identifie les mouvements subis par l'équipement mobile ;
- le gyroscope sert à repérer précisément la position et l'orientation de l'équipement mobile dans l'espace ;
- la géolocalisation permet de connaître les coordonnées géographiques de l'équipement mobile.

La géolocalisation peut s'opérer selon différentes méthodes, parfois utilisées ensemble :

- en cas de connexion à un réseau de communication (Wi-Fi, 3G/4G), l'accès aux informations sur les bornes et les antennes détectées par l'équipement mobile permettent une localisation dont la précision est très variable (de quelques dizaines de mètres à plusieurs kilomètres) ;
- la fonction *GPS* (Global Positioning System) donne un positionnement plus précis, mais qui peut être perturbé à l'intérieur des bâtiments (signaux satellites brouillés).

La fonction géolocalisation de l'équipement mobile requiert pour fonctionner le consentement de la personne et doit apparaître visiblement lorsqu'elle est activée.

7.1.7. Capture multimédia

Les équipements mobiles possèdent souvent sur la face opposée à l'écran un capteur optique (« caméra arrière ») et les équipements mobiles de génération récente ont également un second capteur optique du côté de l'écran (« caméra frontale »), souvent de qualité moindre.

Ces capteurs permettent la prise de photo et la capture vidéo, la caméra frontale pour capter sa propre image avec son environnement du point de vue de l'appareil, et la caméra arrière pour une prise de l'environnement du point de vue de l'utilisateur. Ils permettent la lecture labiale et représentent un excellent outil de compensation de handicap.

Les équipements mobiles possèdent également un microphone permettant l'enregistrement sonore.

Les fichiers résultant de ces outils de capture (images, vidéos, sons) peuvent ensuite être exploités par les applications ayant accès aux données capturées. Les applications pouvant être téléchargées devront respecter le principe de demande d'autorisation préalable de l'utilisateur avant d'accéder à ces fichiers.

7.1.8. Gestion des environnements

Tout comme les ordinateurs de type PC ou Mac, l'utilisation des équipements mobiles pose la problématique de la séparation des données et des usages à titre privé (ou personnel) et professionnel et leur sécurisation.

Une des réponses à ce besoin consiste actuellement en la « containérisation » des usages : des solutions, qui couplées à un outil de gestion de terminaux mobile (Mobile Device Manager ou « *MDM* »), permettent en effet de séparer les applications fournies à titre professionnel de celles installées à titre personnel sur un terminal mobile. Ainsi, il est possible d'empêcher l'utilisation de données manipulées via une application à usage professionnel dans une application dite « personnelle ». À titre d'exemple, il est possible d'empêcher le copier / coller des données d'un mail professionnel vers une application personnelle.

7.2. Gestion des équipements mobiles

Comme pour tout autre matériel informatique, les équipements mobiles nécessitent un processus (et un outil) de gestion de parc. Les objectifs de cette gestion sont :

- garantir la traçabilité du matériel ;
- faire évoluer les solutions logicielles associées selon les besoins ;
- appliquer des règles de sécurité ;
- assurer une certaine qualité de service (par exemple, être en capacité de restaurer rapidement l'environnement de l'utilisateur sur un matériel de remplacement).

Cette gestion repose sur un ensemble de services qui sont potentiellement déjà mis en œuvre pour gérer d'autres types de matériel informatiques (PC fixes, serveurs…).

Ces services présentent toutefois pour les équipements mobiles des spécificités qui seront précisées dans la suite de ce chapitre. C'est pourquoi il existe aujourd'hui des solutions de gestion d'équipement mobile dédiées à ce type de matériel : les *MDM* (Mobile Device Management).

Ces outils utilisent des applications appelées « agent MDM » qui permettent au *MDM* de gérer l'équipement mobile.

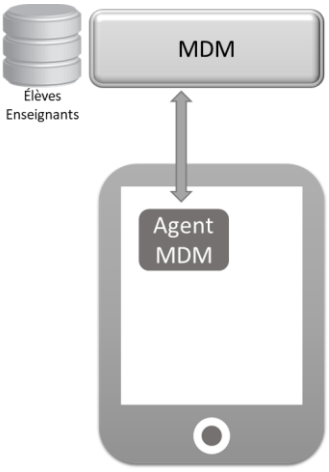


Illustration 8 : Agent MDM

7.2.1. Gestion d'inventaire des équipements mobiles et des accessoires

L'objectif premier de ce service est d'enregistrer les équipements mobiles sur la base d'un identifiant unique (par exemple, le numéro de série ou un tout autre identifiant unique à l'exception de tout numéro de sécurité sociale ou autre identifiant directement lié à une personne) afin de les recenser dans la solution de MxM. Il est important de noter que les données d'identification unique d'un équipement mobile varient en fonction du fabricant du matériel et de l'éditeur du système d'exploitation.

Cet inventaire est à intégrer à l'inventaire général de l'établissement (gestion de parc) afin de pouvoir lier l'équipement mobile avec les accessoires qui lui sont associés, notamment un clavier Bluetooth, un casque audio ou un adaptateur de connectique. Il y a donc une intégration à prévoir entre la solution de MxM et l'outil de gestion de parc informatique global. A minima, les données de référence des équipements mobiles doivent être partagées entre ces outils.

7.2.2. Gestion des profils utilisateur

On parle de « profil utilisateur » pour désigner un ensemble de caractéristiques d'un utilisateur ou communes à plusieurs utilisateurs, dans l'objectif d'assigner des droits ou des contraintes spécifiques relatifs à cet ensemble de caractéristiques.

Ainsi, un même type d'équipement mobile devra être configuré différemment selon, par exemple, qu'il soit utilisé dans le cadre d'une classe mobile avec des terminaux personnalisables ou dans le cadre d'un projet d'EIM mais aussi selon qu'il soit distribué à un enseignant ou à un élève. De façon générale, la caractérisation de ce profil peut se faire sur différents critères qui peuvent être combinés entre eux : élève/enseignant, primaire/collège/lycée, niveau de classe (5e 4e 3e 2de…), matière enseignée, etc.

Les besoins de personnalisation de l'environnement de l'équipement mobile (voir le sous-chapitre suivant « Configuration de mobile ») sont différents selon les profils identifiés ci-dessus.

NB : ces profils existent probablement déjà pour la gestion d'autres matériels informatiques ou pour l'accès à des applications (par exemple l'ENT – Espace Numérique de Travail). Il est possible d'intégrer la solution de MxM avec le système de gestion de ces profils utilisateurs en utilisant le référentiel existant.

7.2.3. Configuration de l'équipement mobile

L'objectif de la configuration est de fournir à l'utilisateur un équipement mobile qui soit le plus possible « prêt à l'emploi », sans manipulation complémentaire de la part de l'utilisateur. Des prestations de service peuvent prendre en charge les adaptations nécessaires.

En effet, une fois acquis, l'équipement mobile va être livré à un endroit défini par son propriétaire (par exemple dans les locaux de la collectivité locale ou de l'établissement). Il y a un certain nombre de tâches à réaliser sur l'équipement mobile avant de le fournir à l'utilisateur « final » et qu'il soit pleinement opérationnel :

- rechargement de la batterie ;
- ajout optionnel d'une carte d'extension mémoire si l'équipement mobile le permet ;
- application des mises à jour du système d'exploitation ; en effet, l'équipement mobile a été empaqueté avec une certaine version du système d'exploitation jusqu'à plusieurs mois avant sa vente, et des mises à jour sont potentiellement disponibles ;
- mise en place de règles de sécurité liées en particulier à l'authentification ; afin de sécuriser l'accès à un équipement mobile, des règles sont à définir sur le déverrouillage de l'équipement mobile par mot de passe, sur le délai de passage en mode veille et du verrouillage associé ; de plus, la désactivation de ces paramètres doit être inhibée afin d'empêcher l'utilisateur de dégrader le niveau de sécurité de l'équipement mobile. Ces règles sont à définir conformément aux recommandations visées ci-avant et notamment celles de l'ANSSI et de la Cnil ;
- création d'un profil local ou application d'un profil utilisateur pour répondre aux besoins du *MDM* selon les choix avec par exemple : mise à jour des paramètres de langue, configuration de l'accès à un serveur de messagerie électronique, à un réseau Wi-Fi, ajout de fond d'écran… ;
- mise à disposition de ressources numériques transverses et/ou spécifiques au profil de l'utilisateur ; il peut s'agir d'installation d'applications ou de chargement de contenu ;
- appairage de l'équipement mobile avec ses accessoires (clavier Bluetooth par exemple) ;
- dans le cas de restitution définitive du matériel (suite à prêt, remplacement, terminal personnalisable…), une solution d'effacement irréversible des données à caractère personnel stockées sur l'équipement doit être prévue. Un transfert de tout ou partie des données à caractère personnel doit être rendu possible.

7.2.4. Application des politiques de sécurité

Le référentiel de sécurité en vigueur doit contenir les règles de sécurité applicables à tous les équipements. Il s'agit de la PSSI (politique de sécurité des systèmes d'information) de l'EPLE ou de l'école (voir le référentiel CARINE).

Les règles de sécurité propres aux équipements mobiles sont à traduire dans l'outil de gestion des équipements mobiles pour leur être appliquées. Les mesures techniques et organisationnelles pour assurer la sécurité des équipements mobiles sont à définir et à appliquer en tenant compte notamment des risques relatifs aux données à caractère personnel.

Parmi les règles à prendre en compte nous pouvons citer :

- chiffrement des mots de passe et des données stockées sur l'équipement mobile, afin d'empêcher l'accès malveillant à des données potentiellement sensibles ;
- bridage de fonctionnalités ; par exemple pour empêcher l'utilisateur de dégrader le niveau de sécurité de l'équipement mobile ;
- contrôle de l'installation et de l'usage d'applications ; création d'une liste noire d'applications interdites ou d'une liste blanche d'applications autorisées ;
- contrôle d'accès aux espaces de partage, pour empêcher par exemple le partage de données sur un nuage non référencé (protection contre la fuite d'information) ;

- accès contrôlé aux données locales, pour empêcher la modification de la configuration du système d'exploitation ;
- restriction de l'usage des équipements mobiles dont l'intégrité du système d'exploitation n'est plus garantie ; il s'agit de terminaux dont le système d'exploitation d'origine a été remplacé par une version permettant une élévation des privilèges pour l'utilisateur et les programmes qui s'y exécutent (débridage) ;
- dans les cas de perte ou de vol, application de règles de sécurité supplémentaires et mise en œuvre de restrictions de l'usage de ces terminaux, jusqu'à la mise en quarantaine du matériel.

Les outils de gestion des équipements mobiles permettent d'effectuer un contrôle sur l'équipement mobile du respect des règles ci-dessus et de déclencher par exemple les actions suivantes :

- émission d'alerte vers le gestionnaire du parc d'équipement mobile ;
- verrouillage et nettoyage d'équipement mobile compromis ;
- réinitialisation de codes d'accès ;
- suppression de données ;
- limitation d'usage de fonctionnalités de l'équipement mobile dans les cas de perte ou de vol.

7.2.5. Monitorage / compte rendu / statistiques des équipements mobiles

Les outils de gestion des équipements mobiles permettent un suivi du parc au moyen des fonctionnalités, plus ou moins riches, avec par exemple :

- mise à disposition de rapports détaillés sur les configurations matérielle et logicielle des équipements mobiles hormis les terminaux BYOD ;
- paramétrage de listes de surveillance pour détecter et recevoir des alertes ;
- identification des vulnérabilités détectées (remontée des équipements mobiles « corrompus », du non-respect des règles de sécurité…) ;
- capacité de recherche avancée sur l'ensemble des données collectées relatives aux caractéristiques ou à l'état des équipements mobiles (pour identifier par exemple tous les terminaux pour lesquels une mise à jour critique du système d'exploitation n'a pas encore été appliquée) ;
- suivi de la consommation data (transfert de données via réseau Wi-Fi) en temps réel des équipements mobiles enrôlés dans le MDM, avec mise en place d'alerte sur seuil. Cette recommandation vaut également pour les terminaux BYOD.

7.2.6. Sauvegarde et restauration des images des équipements mobiles

En cas d'indisponibilité de l'équipement mobile (lors d'une panne, de la perte ou du vol de celui-ci), il est important de pouvoir mettre à disposition de l'utilisateur un nouveau terminal dans les meilleurs délais afin de limiter la durée de rupture de service.

Hormis pour le cas des terminaux BYOD, ceci implique de sauvegarder l'image de l'équipement mobile à intervalle régulier. Par « image » s'entend un ensemble cohérent de la configuration de l'équipement mobile, des applications qui y sont installées et des données qui y sont stockées.

Un processus de restauration de cette image sur un nouvel équipement mobile est à définir. Il peut être suivi d'un processus d'activation. Plus ces opérations sont automatisées, plus l'opération de restauration est rapide et le nouvel équipement mobile fourni au plus vite à l'utilisateur. Dans tous les cas, il s'avère utile de disposer des informations sur la liste des applications installées sur l'équipement (accord préalable de l'utilisateur dans le cas du BYOD).

Les éditeurs de système d'exploitation mobiles ont défini des processus de sauvegarde et de restauration qui sont basés sur des environnements publics en nuage (cloud) pour le stockage des images des équipements mobiles. Cette approche est séduisante pour des usages personnels grand public mais elle peut présenter des limites dans un contexte éducatif ou professionnel :

- les garanties contractuelles peuvent être incompatibles avec ce contexte ;
- les tailles limites de stockage (et les coûts de stockage complémentaires), et parfois les débits, sont à la main de l'éditeur.

Selon les conditions offertes par les éditeurs, il peut donc être nécessaire de définir une solution spécifique pour la gestion de ces images des équipements mobiles.

7.3. Sécurité de l'équipement mobile

Comme pour tout autre matériel informatique, l'usage d'équipement mobile dans un contexte non exclusivement privé implique la mise en place d'un cadre de sécurité pour une bonne utilisation. Les services ci-après sont alors mis en œuvre.

7.3.1. Authentification

Lors de l'accès à des ressources protégées (l'équipement mobile lui-même, les applications installées, les réseaux mis à disposition des utilisateurs dans le domaine éducatif), l'identité de l'utilisateur est vérifiée. Cette authentification de l'utilisateur peut être réalisée à plusieurs niveaux : équipement mobile, réseau, application.

- niveau équipement mobile : les dernières générations d'équipement mobile et les systèmes d'exploitation associés permettent d'authentifier l'utilisateur lors de l'accès à l'équipement mobile via un code d'accès local, une reconnaissance d'empreinte digitale ou faciale (cf. §14.4), voire un schéma d'authentification (technique permettant de dessiner un schéma simple avec le doigt pour déverrouiller l'équipement mobile). Il est possible d'imposer le mode d'authentification via un outil de *MDM* ;
- niveau réseau : accès au réseau Wi-Fi (sécurisé selon la norme IEEE 802.11i) et accès aux systèmes de fichiers réseau ;
- niveau application : l'accès aux applications peut nécessiter a minima une authentification de l'utilisateur gérée par un système central (par opposition au code d'accès local à l'équipement mobile). Ce mécanisme implique une intégration entre l'application et le système d'authentification et peut impacter l'utilisation de l'application en mode non connecté.

NB : les problématiques d'authentification sont traitées dans le S2i2e - CARINE et le référentiel Wi-Fi (cf. chap. 4 « Référentiels connexes et guides »).

7.3.2. Autorisation

Une fois l'utilisateur authentifié, l'usage de certaines fonctionnalités de l'équipement mobile et des applications associées ou l'accès à du contenu peut être fonction du profil de l'utilisateur.

Les *profils* des utilisateurs sont définis et gérés dans des référentiels de type annuaire.

7.3.3. Gestion des annuaires

La solution de MxM s'appuie donc sur un référentiel de données pour contrôler l'usage de l'équipement mobile et l'accès aux ressources numériques depuis le terminal.

7.3.4. Propagation des identités

Comme vu précédemment, la solution de MxM lorsqu'elle est présente permet d'affecter un terminal à un utilisateur et nécessite une association entre des *profils* d'usage des équipements mobiles (définis au niveau du service de gestion des équipements mobiles) et des *profils* utilisateurs venant de référentiels d'identité.

Des données sur les utilisateurs (identités, *rôles* / *profils*) sont donc rendues disponibles ou accédées par la solution de MxM lorsqu'elle est présente. Le mode de transmission (réplication à intervalle régulier, interrogation des référentiels d'identité) est à déterminer en fonction du contexte spécifique à chaque implémentation et doit être sécurisé.

7.3.5. Définition des politiques de sécurité

Comme pour tout autre matériel informatique, des règles de sécurité s'appliquent aux équipements mobiles. Ces règles de sécurité sont définies dans la PSSI de l'EPLE ou de l'école (voir référentiel CARINE). Une partie d'entre elles est commune à tous les types de terminaux ; d'autres ne concernent que certains types d'équipements mobiles seulement.

Ceci a pour objectif de :

- garantir un fonctionnement nominal des terminaux ;
- protéger le système d'information embarqué sur l'équipement mobile (contre les actions malveillantes, virus…) ;
- s'assurer que les règles de sécurité définies sont correctement appliquées (audit…) ;
- limiter au maximum les actions de pirates qui pourraient être réalisées depuis l'équipement mobile vers le système d'information auquel le terminal se connecte, ces actions pouvant être initialisées suite à des actions volontaires ou involontaires de l'utilisateur sur l'équipement mobile (installation de versions altérées d'applications, modification du système d'exploitation).

Il est ainsi pertinent de sécuriser le plus possible l'accès (logique) à l'équipement mobile en définissant des règles applicables aux codes d'accès (type de caractères à utiliser, longueur minimale, durée de vie du code). Un éventuel cryptage des données peut également permettre d'augmenter le niveau de sécurité.

Il convient également de préciser les procédures à appliquer en cas de perte ou de vol de l'équipement mobile, et d'en informer les utilisateurs.

7.3.6. Détection du non-respect des politiques de sécurité

Une fois les politiques de sécurité définies, le contrôle de la conformité de l'équipement mobile est réalisé par l'agent local de la solution de MxM. Cet agent peut permettre selon les solutions :

- la détection du contournement de ces règles sur l'équipement mobile ;
- le déclenchement d'actions sur l'équipement mobile appliquant des restrictions de l'usage de ces terminaux pouvant aller jusqu'à la mise en quarantaine du matériel ;
- l'émission d'alertes à destination des équipes en charge de la gestion des équipements mobiles et plus globalement en charge de la sécurité informatique ;
- l'émission d'alertes à destination du responsable du traitement, notamment en cas de violation de données.

Des outils de protection (par exemple anti-virus) sont installés pour surveiller l'état de l'équipement mobile.

De plus, l'intégrité du système d'exploitation est contrôlée afin d'empêcher des fonctionnements non autorisés des équipements mobiles. Ainsi la modification du système d'exploitation suite à une action de l'utilisateur (débridage par exemple) entraîne des restrictions d'usage (accès réseau / applications désactivées).

Des règles de conformité aux principes sont définies, applicables et contrôlables via le service de gestion des équipements mobiles.

NB : la remise en conformité de l'équipement mobile peut nécessiter dans certains cas la réinitialisation du terminal, pouvant entrainer une perte de données pour l'utilisateur.

7.4. Support matériel

Une assistance de premier niveau offerte aux utilisateurs des équipements mobiles a pour objectif de faire un premier diagnostic du problème rencontré et de préciser les actions de support à mener.

Cette assistance prend globalement la forme d'un support téléphonique pour faciliter les interactions entre l'utilisateur et l'équipe support, accompagné d'un guichet en ligne de traitement des tickets, et d'une aide à l'auto-résolution de problèmes de premier niveau (« autodépannage », foire aux questions).

Les types d'incident matériel peuvent être catégorisés comme suit :

- casse (ex. : chute de l'équipement mobile et bris de la dalle de verre, câble de chargeur sectionné…) ;
- limite matérielle atteinte (ex. : espace disque saturé) ;
- panne (ex. : batterie défaillante) ;
- accessoire inopérant (ex. : problème de configuration) ;
- connectivité réseau hors d'usage (ex. : Wi-Fi inaccessible).

Afin de faciliter le diagnostic et selon la panne, il peut s'avérer utile d'avoir sur les équipements mobiles une solution de prise de contrôle à distance et d'accès aux vues d'écran du terminal. Certains outils de gestion d'équipements mobiles incluent cette fonctionnalité. Celle-ci devra permettre une information de l'utilisateur sur l'équipement mobile et nécessiter un acte positif de sa part. À la fin de la prise de main à distance, un message de fin de session devra s'afficher.

7.5. Classes mobiles

Les classes mobiles sont des conteneurs d'une demi-douzaine à une trentaine d'équipements mobiles mis à disposition d'un ensemble d'élèves (l'équipement n'est donc pas affecté à un élève unique). L'ensemble dispose d'une relative mobilité, la classe mobile pouvant être déplacée d'une salle à une autre, et stockée dans une pièce sécurisée quand elle n'est pas utilisée.

Les conteneurs offrent généralement plusieurs fonctions comme (cette liste n'étant ni exhaustive ni systématique) :

- la sécurisation du matériel ;
- le chargement des terminaux ;
- une borne Wi-Fi intégrée ;
- la possibilité d'imprimer ;
- la projection.

En complément du conteneur et des terminaux, certaines offres intègrent un outil de gestion pour superviser la classe mobile, avec un équipement dédié pour l'enseignant.

Les dispositifs de type « classe mobile » sont plus particulièrement répandus dans le premier degré.

Les équipements mobiles sont rendus disponibles à tous les élèves, selon l'usage identifié par les enseignants et peuvent être utilisés en groupe ou de manière individuelle. La mise à disposition des équipements est également fonction de leur disponibilité, de la situation pédagogique mise en place durant la séance et de l'organisation spatiale de la salle de classe.

Les classes mobiles peuvent être associées à une ou plusieurs classes ou encore dédiées à une activité particulière (projet, domaine d'enseignement, discipline…). Dans l'usage, la classe mobile est de manière générale destinée à être multi-utilisateurs.

Le format des conteneurs et les systèmes d'exploitation des équipements utilisés dans les classes mobiles varient selon les marques et les offres. Les conteneurs se présentent sous forme de valises, de chariots, ou parfois d'armoires.

On identifie 3 principaux modes d'usage :

- les terminaux banalisés. Ils permettent d'accéder à des informations sans aucune personnalisation. L'utilisateur accède aux manuels, aux applications sélectionnées ainsi qu'aux informations génériques ;
- les terminaux à configurations multiples. Ils sont utilisables par des comptes génériques, permettant l'interchangeabilité entre les utilisateurs afin d'accéder à un même niveau d'information et de fonctionnalités ;
- les terminaux personnalisables. L'utilisateur peut s'authentifier sur tous les terminaux. Suite à son authentification, il accède à ses informations configurées sur la base de son profil.

7.6. BYOD / AVEC

Un terminal BYOD est un équipement numérique personnel dont la responsabilité ne relève ni de l'État ni de la collectivité.[16]

Les typologies de terminaux BYOD sont les suivantes :

- mobile multifonction ;
- tablette ;
- mobile hybride ;
- ordinateur portable.

Les téléphones mobiles (non mobile multifonction) et autres objets communicants ne sont pas inclus dans le périmètre.

Dans une démarche BYOD, différentes approches peuvent être suivies selon les choix des porteurs de projet, le périmètre et les modalités de concertation entre partenaires. Selon les cas, il peut s'avérer pertinent de formuler des listes de caractéristiques pour l'acquisition des équipements par les utilisateurs.

Dans le cas d'une approche basée sur des équipements déjà acquis par les utilisateurs, il n'est pas prévu d'accompagnement à l'acquisition des équipements (à l'exception des dispositifs d'aide aux élèves non équipés personnellement) ni de consignes particulières sur leurs caractéristiques et leur mode d'acquisition. Les élèves sont invités à apporter, dans le cadre du projet pédagogique de l'établissement, les équipements dont ils disposent.

En revanche, une approche basée sur l'accompagnement des utilisateurs à l'acquisition de leurs équipements peut conduire à l'expression de caractéristiques pour ces équipements, selon les choix et contraintes pédagogiques ou techniques du projet, ainsi qu'à la mise en place de dispositifs spécifiques pour leur acquisition.

Les éventuels critères de choix relatifs à l'acquisition d'équipements de type BYOD ne sont pas traités dans ce cadre de référence mais le sont dans le guide des projets BYOD.

[16] À consulter le Guide des projets pédagogiques s'appuyant sur le BYOD/AVEC version V1.2 (eduscol.education.fr/cid128686/guide-des-projets-pedagogiques-s-appuyant-sur-le-byod-avec.html).

Dans le cas des 2 approches, il est nécessaire de :

- s'assurer de la disponibilité de l'infrastructure et des prérequis techniques permettant aux équipements d'accéder aux services et fonctionnalités mis en place par l'établissement ;
- veiller à mettre en place des solutions d'accompagnement spécifiques.

La prise en compte du BYOD vient compléter le périmètre des équipements disponibles. Trois types d'équipements sont donc à considérer : les EIM, les classes mobiles d'équipements mobiles et les équipements BYOD.

De ce fait, la question du périmètre de gestion de parc se pose : y a-t-il intérêt à intégrer les équipements personnels à la gestion de parc dans le cadre d'un projet BYOD ?

Deux options se présentent :

- option 1 : La gestion de tout le parc d'équipements y compris les équipements BYOD :

  Dans ce cas de figure, les élèves ou leurs responsables légaux installent un client MxM sur leur équipement BYOD, cédant ainsi le contrôle de l'équipement à la collectivité ;
- option 2 : La gestion de parc d'équipements ne comprend pas les équipements BYOD :

  Cette option consiste à sécuriser les équipements via une défense en profondeur des systèmes d'information et services mis en place au sein des établissements au lieu de recourir à une solution de gestion de parc.

Les avantages et les inconvénients de chacune de ces deux options sont bien détaillés dans le guide des projets pédagogiques s'appuyant sur le BYOD/AVEC.

7.7. Gestion du cycle de vie des équipements mobiles et des accessoires

La mise à disposition d'équipements mobiles est un projet de déploiement d'équipement informatique (hormis dans le cas de projets BYOD) qui s'exécute selon six étapes.

Illustration 9 : Cycle de vie des équipements mobiles et accessoires

Ce projet ne se limite pas à un simple déploiement de matériel. Il doit s'inscrire dans un programme plus complet incluant la sélection et la mise à disposition de ressources numériques. C'est cet ensemble qui permet de répondre pleinement aux besoins utilisateurs.

7.7.1. Planification

Cette phase sert à définir le cadre du projet sur les thématiques suivantes :

- l'équipe : quelles sont les parties prenantes du projet (collectivités locales, représentants d'établissement, direction informatique académique…) ? Quel est leur rôle (maîtrise d'ouvrage / porteur de projet, maîtrise d'œuvre / réalisation de projet, achat…) ?
- le périmètre : quelles sont les populations d'utilisateurs ciblées (*profils*, nombre) ? Quels sont les usages à couvrir (besoins fonctionnels) ? Quelles sont les contraintes techniques associées (intégrations au niveau réseaux et sous-systèmes du système d'information, normes de sécurité, compatibilité avec les ressources numériques devant être utilisées via l'équipement mobile…) ?
- les dépendances : quels sont les autres projets liés à la réussite du déploiement des équipements mobiles (mise en place de réseau Wi-Fi, sélection de l'outil de gestion des équipements mobiles, des ressources numériques répondant aux usages, aménagement de points de recharge…) ? Comment pilote-t-on la synchronisation de ces projets ?

- la dimension financière : quelle est l'enveloppe budgétaire allouée au projet ? Quels sont les coûts de mise en œuvre du projet (acquisition, fonctionnement) ?
- le planning : quelles sont les principales échéances du projet (périodes d'exécution des phases décrites ci-après) ?

7.7.2. **Acquisition**

Une fois les éléments de cadrage identifiés lors de la phase de planification, le processus d'acquisition des équipements mobiles se déroule classiquement comme suit :

- rédaction et publication de l'appel d'offres (il peut y avoir plusieurs appels d'offres distincts entre les équipements mobiles et les accessoires) ;
- analyse et évaluation des réponses ;
- le cas échéant, soutenances des répondants retenus sur dossier ;
- finalisation des négociations commerciales et contractualisation avec le ou les fournisseurs retenus.

7.7.3. **Préparation**

Cette phase regroupe les activités qui sont réalisées avant de fournir l'équipement mobile et ses accessoires à l'utilisateur final ou à l'établissement :

- lotissement du déploiement effectif en fonction du planning de livraison des fabricants ;
- référencement des matériels au niveau de l'outil de gestion des équipements mobiles et de la gestion de parc du propriétaire, association équipement mobile / accessoires ;
- affectation des EIM aux utilisateurs finaux ;
- configuration des équipements mobiles (appairage d'accessoires, chargement de la batterie, ajout de carte mémoire *SD*) ;
- enrôlement dans son environnement d'utilisation, paramétrage (ex : Wi-Fi) ;
- configuration du conteneur de classe mobile le cas échéant ;
- application des règles de sécurité ;
- installation des ressources numériques cibles ;
- établissement de la cellule de support ;
- planification de la mise à disposition (distribution) aux utilisateurs finaux ;
- rédaction des documents de mise à disposition (cf. §21.2.6).

Les projets connexes (mise en œuvre de réseau Wi-Fi, mise en production des composants du système d'information nécessaires à l'utilisation des ressources numériques) sont finalisés en parallèle de cette phase de préparation.

7.7.4. **Distribution**

Dans cette phase, l'utilisateur final se voit remettre son EIM (dans le cas d'un projet d'EIM) ou l'établissement se voit remettre ses équipements mobiles (dans le cas d'un projet de classes mobiles). Éventuellement, des accessoires sont aussi distribués dans cette phase.

Cette phase peut inclure plusieurs activités :

- signature d'un « bon de remise » pour signifier que l'utilisateur a pris possession de son EIM et de ses accessoires ou que l'établissement a pris possession de ses équipements mobiles et de ses accessoires ;
- aide à la prise en main de l'équipement mobile ;
- distribution ou rappel de la charte d'utilisation.

7.7.5. **Utilisation**

Une fois les équipements mobiles distribués, commence la phase opérationnelle de mise en œuvre de la solution (« service régulier »). Durant celle-ci, les activités suivantes seront conduites sous la responsabilité des parties prenantes :

- support matériel ;
- suivi d'incidents (sur la base du pilotage de la cellule support et du compte rendu de ses interventions) ;
- gestion de l'équipement mobile (mise à jour du système d'exploitation, réaffectation…) ;
- audit de l'application des règles de sécurité ;
- analyse des retours d'expérience sur les usages, capitalisation sur les bonnes pratiques et identification des axes d'amélioration ;
- identification et priorisation des besoins d'évolution (par exemple évolution des politiques de sécurité) ;
- suivi budgétaire.

7.7.6. **Mise au rebut**

Une fois que l'équipement mobile est reconnu obsolète, le processus de décommissionnement est défini :

- suppression sécurisée des données (de configuration et potentiellement de l'utilisateur) ;
- désinstallation des applications ;
- sortie d'inventaire ;
- revente ou don du matériel ou envoi à un tiers pour destruction selon les normes en vigueur (recyclage et traitement des matières dangereuses pour la santé).

Chacune de ces étapes doit faire l'objet d'une journalisation afin de pouvoir démontrer à tout moment que l'opération s'est faite de manière sécurisée et confidentielle.

Du fait de l'évolution des matériels, des systèmes d'exploitation et des standards technologiques associés, les équipements mobiles sont rapidement obsolètes (par expérience entre 3 et 5 ans après leur mise sur le marché).

Note : en cas de perte ou de vol de l'équipement mobile, les procédures prévues par la politique de sécurité sont appliquées.

7.7.7. **Renouvellement du cycle**

Le parc des équipements mobiles est ainsi géré de manière itérative. Un projet de renouvellement est initialisé pendant la phase d'utilisation des équipements mobiles sélectionnés lors du projet précédent. Ce nouveau projet tire parti des enseignements capitalisés pendant le projet précédent.

Le cycle de vie des accessoires n'est généralement pas le même que celui des équipements mobiles. Le renouvellement des accessoires fait l'objet d'une gestion spécifique.

8. Présentation des fonctions : ressource numérique

La première partie (§ 8.1) de ce chapitre propose les typologies permettant de classer les ressources numériques accédées par les utilisateurs, selon une classification fonctionnelle ou technique.

Sont ensuite précisés les grands principes de gestion des ressources lorsqu'il s'agit d'applications mobiles (distribution, support et cycle de vie).

8.1. Typologies fonctionnelles et techniques

8.1.1. Classement des services fonctionnels

D'un point de vue fonctionnel, les ressources numériques déployées sur l'équipement mobile ou accessibles via l'équipement mobile ont pour objectif de contribuer à la réalisation des usages par l'utilisateur. La classification ci-dessous reprend en partie celle du SDET.

- Services de communication et de collaboration :
  - messagerie (courrier) électronique ;
  - espaces d'échanges et de collaboration (ex : forums, blogs) ;
  - messagerie instantanée ;
  - affichage d'informations ;
  - conférence audio et vidéo ;
  - …
- Services informationnels et documentaires :
  - carnet d'adresses ;
  - service d'agendas ;
  - pages blanches ;
  - service de recherche ;
  - gestion des signets ;
  - accès aux ressources pédagogiques éditoriales ;
  - gestion des activités documentaires ;
  - …
- Services d'accompagnement de la vie de l'élève :
  - cahier de textes / cahier journal ;
  - suivi individuel des élèves ;
  - affichage de l'emploi du temps ;
  - cahier de liaison / de correspondance ;
  - …
- Services de production pédagogique et éducative :
  - outils audio / vidéo ;
  - outils de création de contenu multimédias ;
  - outils bureautiques ;
  - construction et gestion de parcours pédagogiques ;
  - …

Tout en n'étant pas spécifiques aux équipements mobiles, les services de gestion de classe offrent à l'enseignant des facilités pour administrer une classe d'élèves travaillant sur des terminaux informatiques.

- Services de gestion de classe[17] :
  - diffusion d'un document à l'ensemble de la classe et ramassage de documents ;
  - autorisation ou restriction des accès aux ressources en fonction des objectifs pédagogiques de la séquence ;
  - visualisation de l'écran des élèves sur le poste de l'enseignant ;
  - affichage de ce que fait un élève sur les équipements mobiles d'autres élèves ou sur un écran collectif ;
  - mise en place d'enquêtes ;
  - création de groupes de travail virtuels ;
  - diffusion d'un fichier audio ou vidéo à tous les élèves ou à un groupe ;
  - blocage/autorisation de copie de données depuis ou vers un périphérique de type carte *SD* ou clé USB ;
  - blocage d'écrans à distance (en plus du partage d'écrans) ;
  - blocage/autorisation d'applications ;
  - consultation de la liste des équipements mobiles de la classe ainsi que leur état (batterie, connectivité…) ;
  - blocage/autorisation d'utilisation de périphériques (clé USB, clavier) ;
  - sessions de discussion (messagerie instantanée) ;
  - utilisation du micro (l'enseignant parle aux élèves, ou les écoute en les en informant préalablement) ;
  - …

8.1.2. Typologies techniques

Ce chapitre propose de différencier les applications selon deux angles d'approche :

- selon l'emplacement (local ou distant) des services et des contenus ;
- selon leur technologie.

8.1.2.1. Selon l'emplacement des services et contenus

- Dans le cas où le service est sur l'équipement mobile il convient d'installer une application mobile. Le contenu peut être soit également sur l'équipement mobile, soit distant.
- Dans le cas où le service est distant on parle alors de ressource numérique en ligne. Le contenu est également distant.

[17] Ces services sont également évoqués au chapitre 17

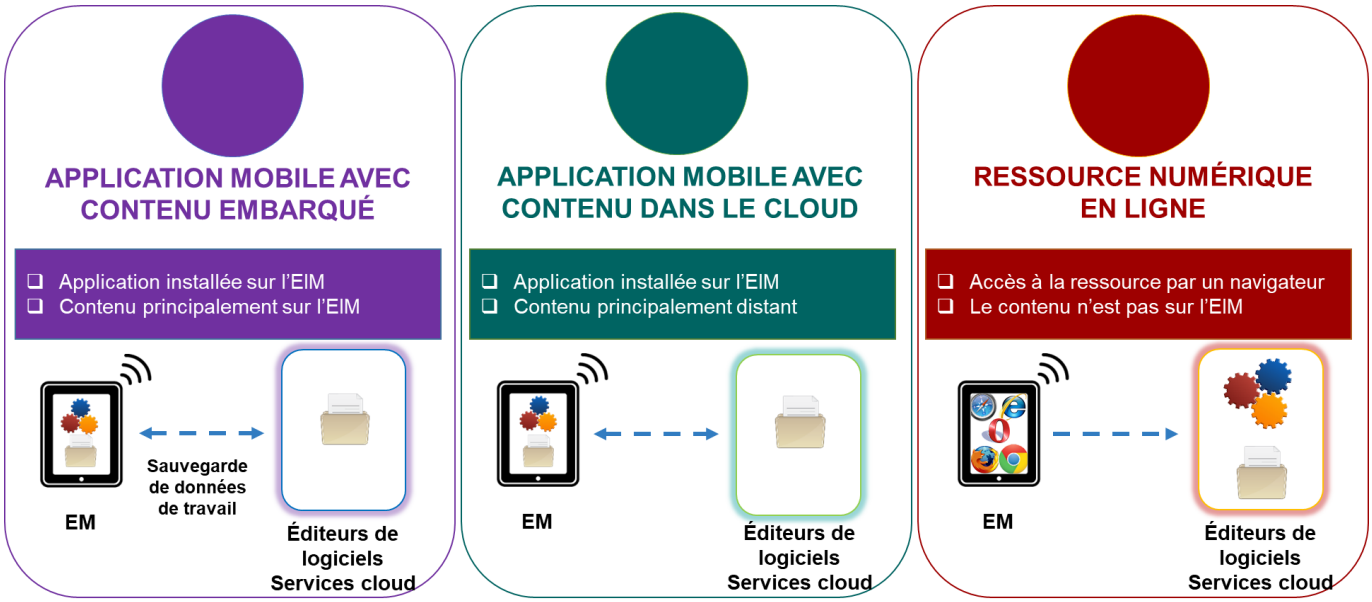


Illustration 10 : Typologie d'applications mobiles selon l'emplacement des services et contenus

8.1.2.2. Selon leur technologie

On distingue les **applications mobiles**, « natives » ou « hybrides », et les **applications web** mobiles.

A. Les applications mobiles

Les applications déployées sur les équipements mobiles peuvent fonctionner selon trois modes :

- en mode déconnecté : l'application n'utilise jamais le réseau ;
- en mode connecté : l'application ne fonctionne pas sans réseau ;
- fonctionnement possible en mode déconnecté : pour certaines opérations ne nécessitant pas d'échange d'information, il est possible d'utiliser l'application en mode déconnecté (pour une synchronisation, le cas échéant, lorsque le réseau est à nouveau disponible).

a) Les applications mobiles « natives »

Ces applications sont développées pour un système d'exploitation spécifique. Elles peuvent accéder via les API[18] du système d'exploitation à l'ensemble des caractéristiques de l'appareil, dont par exemple l'appareil photo, les capteurs (*GPS*, accéléromètre et boussole inclus), la liste des contacts.

Les applications natives sont téléchargeables depuis un magasin d'applications.

[18] API (Application Programming Interface) désigne une interface applicative de programmation par laquelle un logiciel offre des services à d'autres logiciels.

Illustration 11 : Applications mobiles « natives »

b) Les applications mobiles « hybrides »

Une application mobile hybride est une application mobile développée dans un conteneur compatible avec différentes plateformes, et qui peut donc être déployée sur plusieurs systèmes d'exploitation.

Les applications mobiles hybrides peuvent s'appuyer sur plusieurs des caractéristiques disponibles de l'appareil, avec toutefois des possibilités plus limitées qu'une application native ; elles sont téléchargeables depuis un magasin d'applications.

Illustration 12 : Applications mobiles « hybrides »

B. Applications web mobiles

Dans le cas des ressources numériques en ligne, il n'y a pas de distribution à assurer sur l'équipement mobile ; au mieux, un lien vers le site web peut être ajouté sous forme de favori du navigateur utilisé sur l'équipement mobile ou d'un raccourci (icône) sur le bureau de l'équipement mobile. On parle **d'applications web mobiles**.

Il s'agit de sites web qui ressemblent fortement à des applications mobiles.

Les applications web mobiles peuvent être conçues en HTML5 comme des applications à page unique, et simuler le déplacement d'une page à l'autre à l'aide d'ancrages HTML. Ces applications fonctionnent dans un navigateur de l'appareil, mais il se peut qu'il n'y ait aucune barre, ni bouton de navigateur, et il devient alors difficile de les distinguer d'une application hybride ou native.

Les utilisateurs accèdent à l'application en navigant vers une URL et peuvent ajouter un signet à cette page sur le navigateur de leur appareil.

Ces applications fonctionnent en mode connecté, c'est-à-dire que le contenu de l'application est récupéré sur le réseau via un navigateur (une connexion réseau est préférable pour en permettre un fonctionnement optimal, même si un fonctionnement avec du cache local est parfois possible).

Illustration 13 : ***Applications web mobiles***

8.2. Distribution des applications mobiles

Les applications mobiles sont disponibles sur des magasins appelés stores. Les droits d'usage peuvent être acquis sur le store lui-même ou sur des plateformes de distribution.

On désigne par *MAM* (Mobile Application Management) les fonctions utilisées dans le cadre de gestion de flottes d'équipements mobiles pour gérer les applications acquises. On parle aussi de gestionnaire d'applications.

Ce gestionnaire d'applications propose quatre principales fonctions :

- inventaire du parc applicatif ;
- association entre les applications et les utilisateurs ;
- distribution des applications ;
- supervision de données relatives aux applications.

Le gestionnaire d'applications gère également la distribution des applications en respectant le nombre de licences achetées. On parle alors de nombre de jetons acquis. Certaines applications disposent de leur propre système de gestion des droits indépendamment du nombre d'applications distribuées par le MAM.

Les applications pouvant être installées sur l'équipement mobile doivent être configurées dans le respect des principes légaux de proportionnalité et de minimisation des données. Ces derniers impliquent de vérifier que les données traitées ou accédées sont adéquates, pertinentes et limitées à ce qui est nécessaire aux finalités et aux usages desdites applications.

Ce chapitre aborde plus en détail le fonctionnement des stores ainsi que les différentes fonctions du *MAM* (flèches vertes dans le schéma ci-après).

Notons qu'il est possible pour un équipement mobile de gérer seul ses applications en se connectant directement au store (flèche bleue dans le schéma ci-après) ou chez l'éditeur de l'application ou un de ses distributeurs. Il faut alors que l'utilisateur ait le droit d'installer des applications de manière autonome.

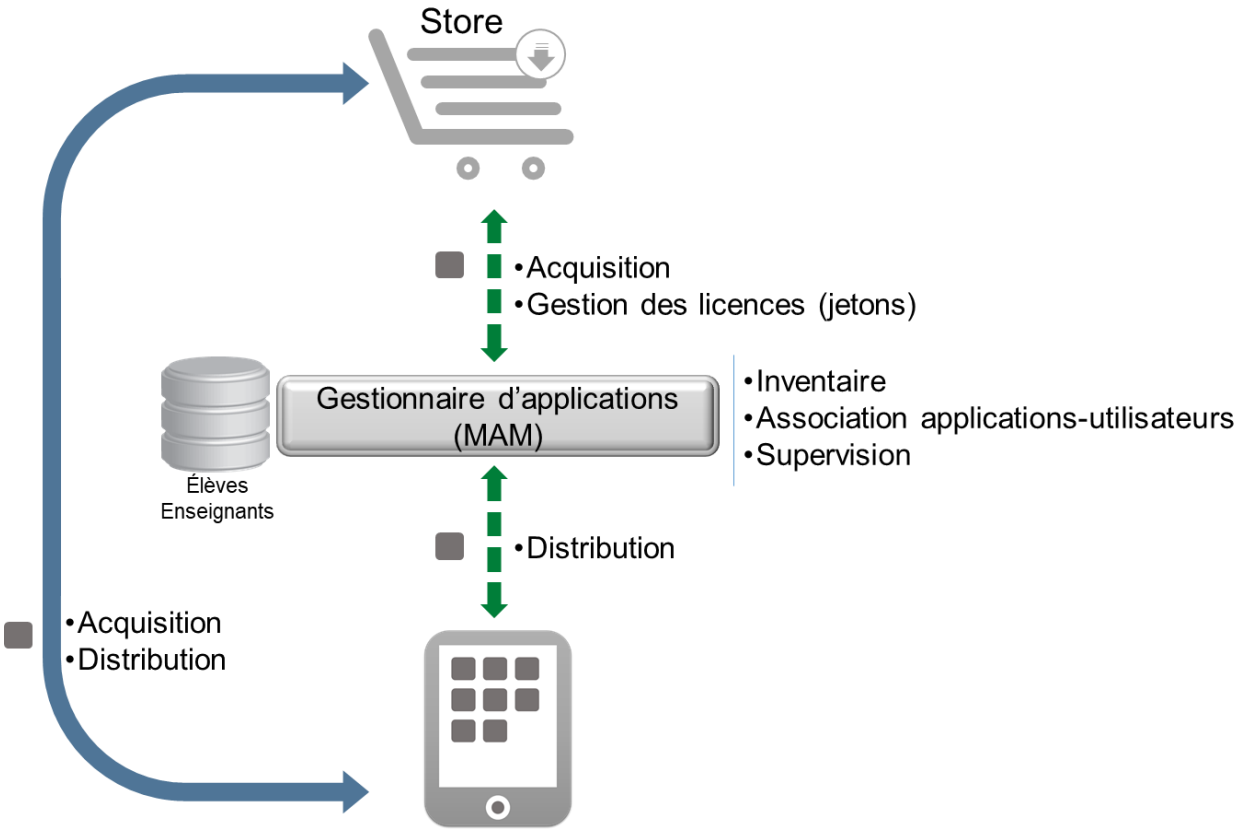


Illustration 14 : Distribution d'applications mobiles

La méthode de distribution des applications décrite dans ce chapitre peut différer dans le cadre des projets BYOD qui n'ont pas recours à une solution de MxM.

8.2.1. Magasin (Store) / Portail d'accès aux ressources

Une standardisation du mode de distribution des ressources de type application mobile s'est faite autour du modèle décrit ci-dessous.

Chaque éditeur de systèmes d'exploitation orienté mobile met en place un « store » de référencement des applications mobiles associées à sa plate-forme. Ce sont des **stores publics**. Ces stores peuvent proposer des rubriques spécifiques « ludo éducation ».

Système d'exploitation	Éditeur	Store
Android	Google	Google Play
ChromeOS	Google	Chrome Web Store
iOS	Apple	App Store
Windows	Microsoft	Windows Store

Tableau 3 : Principaux stores publics

Un store se présente sous la forme d'une application mobile pré embarquée sur l'appareil, ou d'un portail accessible via internet, qui recense les applications disponibles pour des équipements mobiles en donnant des informations sur les fonctionnalités, sur l'éditeur, les appréciations d'autres utilisateurs.

Les éditeurs de ressources y publient leurs applications selon les normes définies par le propriétaire du store (il y a un processus de validation plus ou moins contraignant pour qu'une ressource soit disponible sur le store). Le téléchargement d'une application est réservé aux détenteurs de terminaux embarquant le système d'exploitation correspondant (il n'est par exemple pas possible de télécharger une ressource iOS sur un terminal sous Android).

Le téléchargement de l'application peut être gratuit ou soumis à un achat de licence (dans ce second cas, le propriétaire du store reverse une partie du prix de vente à l'éditeur).

Ces stores étaient initialement destinés au grand public. Dans ce contexte, les achats d'application sont réalisés unitairement par le propriétaire du terminal concerné au moyen par exemple de sa carte bancaire (associée à son compte utilisateur sur le store).

Avec l'utilisation des terminaux mobiles dans le monde professionnel, les éditeurs de store ont intégré la possibilité de faire des achats en volume sur un compte professionnel[19] Ainsi, une entreprise peut effectuer un achat groupé de jetons d'une même application au travers d'un *MAM*. Ses employés utilisent ensuite ces jetons pour obtenir la ressource sur leur terminal.

Un éditeur peut également publier une application personnalisée pour un client professionnel. L'application est dans ce cas publiée sur une **zone privée du store public** réservé à ce client professionnel.

Le modèle ci-dessus concerne les ressources commercialisées (gratuitement ou non pour le volet installation) par des éditeurs.

Une entreprise ou un organisme peut développer ses propres applications à usage purement interne. Dans ce cas, la distribution de ces applications sur les terminaux des employés de l'entreprise ou de l'organisme (que le terminal soit le terminal personnel de l'utilisateur ou celui fourni par l'employeur) peut se faire au travers d'un **store privé** (appelé également store d'entreprise).

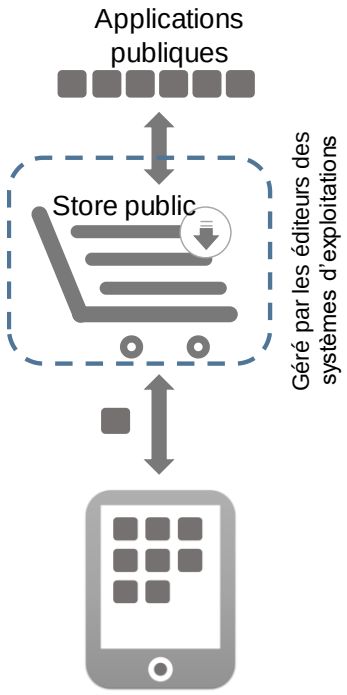
Enfin, pour optimiser l'expérience de l'utilisateur, il est possible de distribuer l'ensemble des applications mobiles via une fonction de *MAM* gérée en interne. L'administrateur du *MAM* peut récupérer des jetons d'applications qui ont été acquises sur un store public et les distribuer sur les équipements mobiles depuis la solution de *MAM* interne. L'utilisateur n'a de cette façon pas besoin de se rendre sur un store public pour accéder aux ressources.

Par ailleurs, la distribution peut également être assurée directement par l'éditeur de l'application ou par un distributeur.

Nous proposons ici une synthèse de ces différents types de store et de leurs caractéristiques :

[19] Chez Apple, il s'agit du programme d'achat en volume : https://www.apple.com/fr/education/it/vpp

8.2.1.1. Store Public



CARACTÉRISTIQUES

- Les éditeurs déposent leurs applications (gratuites ou payantes)
- Les applications sont accessibles à tout le monde

AVANTAGES

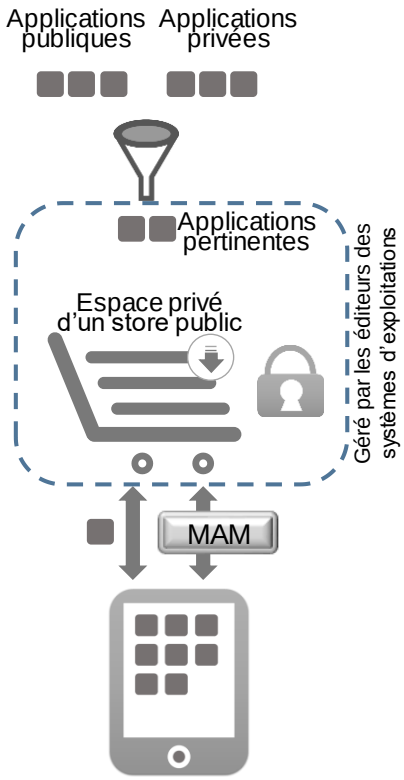
- Tout est géré par l'éditeur du système d'exploitation (Apple, Google, Microsoft, …)

INCONVÉNIENTS / CONTRAINTES

- L'entreprise ou l'organisme ne dispose pas des moyens de maitrise de ce qui est téléchargé

Illustration 15 : Store public

8.2.1.2. Espace privé dans un store public



CARACTÉRISTIQUES

- Les éditeurs déposent leurs applications soit pour le grand public soit à destination de l'espace privé
- Les applications choisies dans l'espace privé sont accessibles aux seules personnes autorisées
- L'accès au store peut être géré par un MAM ou en direct par les utilisateurs

AVANTAGES

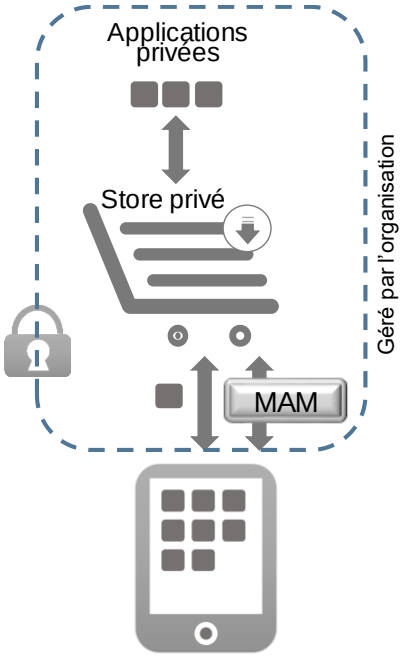
- Seules les ressources pertinentes sont proposées
- L'accès est sécurisé (autorisation accordée selon le compte de l'utilisateur)

INCONVÉNIENTS / CONTRAINTES

- Pour une entreprise il faut autant d'espaces privés qu'il y a d'EIM dont les systèmes d'exploitation sont différents

Illustration 16 : Espace privé dans un store public

8.2.1.3. Store privé (ou store d'entreprise)



CARACTÉRISTIQUES

- Les éditeurs déposent leurs applications à destination de l'espace privé
- Les applications choisies dans l'espace privé sont accessibles aux seules personnes autorisées
- L'accès au store est géré par un MAM ou en direct par les utilisateurs

AVANTAGES

- Seules les ressources pertinentes sont proposées
- L'accès est sécurisé
- Le store privé peut proposer des applications à destination de plateformes différentes

INCONVÉNIENTS / CONTRAINTES

- Nécessité de gérer le store en propre

Illustration 17 : Store privé (ou store d'entreprise)

Signalons enfin qu'une application peut être installée en poussée (push) ou tirée (pull). Dans le mode tiré (pull), l'utilisateur choisit une application et l'installe sur l'équipement mobile qu'il utilise. Dans le mode poussé (push), c'est le gestionnaire d'applications qui va installer l'application sur l'équipement mobile, avec ou sans intervention de l'utilisateur.

8.2.2. Gestion d'inventaire des applications mobiles

L'inventaire des applications mobiles consiste à visualiser toutes les applications présentes dans l'organisation et leur statut : gratuite ou payante, version, historique des mises à jour.

Les applications sont répertoriées dans le *MAM* : identification des versions d'applications utilisées, des systèmes d'exploitation compatibles, recensement des jetons acquis auprès de l'éditeur. Seules les applications gérées dans le *MAM* sont présentes dans l'inventaire.

Un second objectif est de définir des configurations logicielles (*master* applicatif) pouvant être utilisées lors de la préparation des équipements mobiles. Une configuration pouvant être fonction de *profils* utilisateurs ; par exemple la configuration A est à destination des équipements mobiles des enseignants d'un établissement, alors que la configuration B est à destination des élèves de niveau N d'un autre établissement. La configuration peut également être fonction du modèle de l'équipement mobile, notamment du système d'exploitation.

Au-delà des configurations servant à l'initialisation des équipements mobiles, le système de gestion prend en compte les applications acquises au fil du temps.

8.2.3. Monitorage / compte rendu / statistiques des applications distribuées

L'objectif est ici de tenir à jour un certain nombre d'informations sur l'utilisation des applications mobiles au moyen de l'outil de gestion d'applications :

- nombre de jetons utilisés par application ;

- versions déployées des applications ;
- statistiques d'utilisation.

Ces données sont utilisées pour :

- anticiper les besoins d'acquisition de jetons supplémentaires ou au contraire de réaffectation de jetons entre les équipements mobiles (par exemple plus de jetons disponibles pour installer une application sur un équipement mobile alors que la même application installée sur un autre équipement mobile n'est jamais utilisée) ;
- mesurer les impacts d'une montée de version de système d'exploitation (y a-t-il des versions d'application incompatibles avec une nouvelle version de système d'exploitation ?).

8.2.4. Affectation ressource / profil équipement mobile et/ou profil utilisateur

Une fois une application mobile acquise et référencée dans le gestionnaire d'applications, une opération d'affectation est à réaliser entre cette application et des *profils* utilisateur (voire des utilisateurs nominativement) et/ou à des types d'équipements mobiles (en fonction du système d'exploitation compatible ou d'autres caractéristiques techniques comme une taille d'écran, l'existence d'un capteur particulier).

8.3. Support logiciel

L'acquisition, la distribution et l'utilisation des applications mobiles sont souvent accompagnées d'un support logiciel pour résoudre les différents problèmes qui peuvent survenir (impossibilité de télécharger l'application, l'application ne veut pas démarrer…).

L'assistance de premier niveau offerte aux utilisateurs des équipements mobiles a pour objectif de faire un premier diagnostic du problème rencontré et de préciser les actions de support à mener.

Cette assistance prend généralement la forme d'un support téléphonique, pour faciliter les interactions entre l'utilisateur et l'équipe d'assistance.

Les types d'incident logiciel remontés au support peuvent être catégorisés comme suit :

- bogue de l'application ;
- mauvaise manipulation de l'utilisateur / méconnaissance des fonctionnalités ;
- ressources matérielles contraintes (espace disque saturé) ou inopérantes (problème d'accès au réseau Wi-Fi) ;
- systèmes distants inaccessibles (serveur ou réseau en panne) ;
- accès à l'application ou à une ressource associée refusé (problème de configuration ou de droit).

Une assistance de second niveau est généralement nécessaire pour répondre aux cas non résolus précédemment : appel à l'éditeur de l'application ou son distributeur, au constructeur de l'équipement mobile, au store… - les situations sont diverses.

8.4. Gestion du cycle de vie des ressources numériques

Les ressources numériques sont soumises à différents types de licences.

Leur nombre important rend la gestion du cycle de vie primordiale afin de mieux préparer leur acquisition (versus les bons d'achat et le budget alloué) et leur fin/renouvellement de contrat.

Cette gestion implique un suivi de l'obsolescence fonctionnelle (pertinence du choix de l'application) et technique (compatibilité avec le parc d'équipements mobiles).

Les ressources numériques suivent les étapes suivantes :

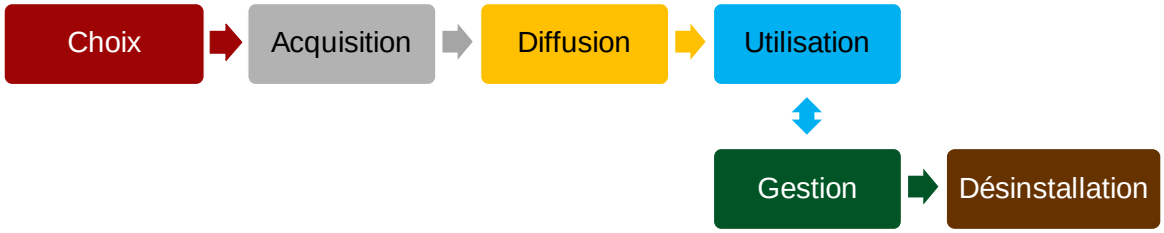


Illustration 18 : Cycle de vie des ressources numériques

8.4.1. Le choix

Cette étape correspond à la sélection réalisée par le prescripteur. Ce choix repose sur plusieurs éléments :

- des éléments descriptifs qui éclairent sur l'intérêt pédagogique de la ressource. Les informations sont apportées par le distributeur commercial de la ressource ou par des retours utilisateurs ;
- des éléments techniques pour valider que la ressource est utilisable par les équipements mobiles qui y accéderont.

8.4.2. L'acquisition

Une fois le choix réalisé, le gestionnaire du compte établissement ou école procède à l'acquisition de la ressource en utilisant les droits de tirage ou subventions associés au compte.

8.4.3. La diffusion

Après l'acquisition, la ressource est disponible pour être associée à des utilisateurs ou des groupes. Le résultat est le déploiement de la ressource sur les équipements mobiles concernés.

8.4.4. L'utilisation

L'utilisateur de l'équipement mobile accède et manipule la ressource.

8.4.5. La gestion

Durant la phase d'utilisation la ressource est amenée à évoluer par le biais de mises à jour effectuées par le distributeur de l'application sur le magasin d'applications. Cette mise à jour sur l'équipement mobile peut être manuelle ou automatisée.

Par ailleurs le prescripteur vérifie que la ressource correspond toujours à un besoin pédagogique et que techniquement l'évolution du parc d'équipements mobiles est compatible avec les caractéristiques techniques de la ressource.

8.4.6. **La désinstallation**

La désinstallation peut être motivée par plusieurs raisons : un départ de l'école ou de l'établissement, la ressource n'a plus d'intérêt pédagogique, une autre ressource lui est préférée, l'évolution du parc d'équipements mobiles fait que la ressource n'est utilisable que par très peu d'utilisateurs…

9. Présentation des fonctions : utilisateurs et accès aux ressources

9.1. Sécurité des accès et référentiels associés

Au-delà des ressources en accès libre, un contrôle d'authentification de l'utilisateur et d'autorisation d'accès est nécessaire lors de l'utilisation d'une ressource.

Ce contrôle peut être effectué de façon locale ou distante.

- Distante : un service distant assure (directement ou indirectement) le contrôle d'accès à partir d'informations communiquées par l'application utilisant la ressource.
- Locale (c'est-à-dire sur un espace de stockage de l'équipement mobile dédié à l'application) : c'est l'application et le système d'exploitation du terminal qui contrôlent l'accès à la ressource. L'application évalue par exemple un code saisi pour autoriser ou non l'accès.

Précisions sur le contrôle distant

L'authentification de l'utilisateur se fait auprès d'un référentiel d'identité.

Le contrôle d'autorisation d'accès d'un utilisateur à une ressource est quant à lui réalisé au travers d'un rapprochement entre un rôle applicatif et un profil utilisateur.

Il y a différentes façons de réaliser ces contrôles d'authentification et d'autorisation d'un utilisateur dans une application :

- via un compte détenu par l'éditeur (qui peut être vérifié à chaque accès ou non) ; cela nécessite un référentiel d'identité porté par l'éditeur pour gérer les comptes ;
- via un code d'activation fourni par l'éditeur ;
- via un contrôle d'accès à l'ensemble des applications assuré par un compte unique utilisateur ; cela implique la mise en place d'un système d'authentification-autorisation central ; les applications y accèdent alors au moyen d'API standardisées.

Afin d'optimiser l'expérience utilisateur (en évitant que celui-ci ait à rentrer ses identifiants/mot de passe lors de l'accès à chaque application), il est également possible de mettre en place un mécanisme d'authentification unique (SSO pour Single Sign-On en anglais) : « *Les technologies fournissant des SSO utilisent des serveurs centralisés d'authentification que toutes les autres applications et systèmes utilisent pour l'authentification, combinant ceux-ci avec des techniques logicielles pour s'assurer que les utilisateurs n'aient pas à entrer leurs identifiants plus d'une fois.* ».

Précisons également qu'un utilisateur déjà authentifié sur une application ne doit pas nécessairement se réauthentifier à chaque ouverture de l'application. Le niveau de sécurité de l'application oblige ou non à se réauthentifier à chaque ouverture.

9.2. Services d'infrastructure pour l'établissement

L'utilisation d'un équipement mobile en établissement et hors établissement nécessite la mise en œuvre de services d'infrastructure associés aux établissements.

9.2.1. Gestion des systèmes informatiques (infogérance serveurs et composants réseaux)

Les services de mobilité s'appuient sur des éléments du système d'information (annuaire utilisateurs…) dont les ressources logicielles et matérielles (serveurs physiques, middleware, systèmes de stockage, routeurs…) sont mises en œuvre et administrées pour répondre à des objectifs de qualité de service.

9.2.2. Services réseau

L'infrastructure Wi-Fi et les débits du réseau local et d'internet sont déterminants dans le succès de la mise en place d'équipements mobiles.

La fiabilité de cette infrastructure est cruciale pour rendre un service constant à l'utilisateur.

Dans le cas des projets BYOD, une attention particulière devra être portée au bon dimensionnement de l'infrastructure Wi-Fi.

De même l'accès aux ressources distantes ou aux productions numériques nécessitent un transfert de l'information fiable et sécurisé.

Les préconisations liées aux services réseaux sont décrites dans le référentiel S2I2E – CARINE et complétées par le référentiel Wi-Fi et le guide BYOD.

9.2.3. Monitorage / compte rendu / statistiques de l'infrastructure

Des services de monitorage permettent de superviser l'état des ressources matérielles (qualité du Wi-Fi, saturation des serveurs…) et de réagir rapidement à des événements inattendus. Un problème sur l'infrastructure peut engendrer une baisse ou une perte de service et pénaliser les usages.

Il faut ainsi prévoir une supervision des infrastructures permettant d'identifier les intrusions ou activités anormales.

Ces activités de monitorage s'imposent pour détecter toute violation de données à caractère personnel qui doivent être notifiées à la Cnil dans un délai de 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Il est précisé que lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

Le compte rendu permet de contrôler et anticiper des dépenses à venir (augmentation des capacités, rajout d'un répéteur Wi-Fi…). Parmi les éléments statistiques qui peuvent s'avérer utiles pour des activités de dimensionnement, figure l'utilisation de la bande passante Wi-Fi par les équipements mobiles. Cette information peut être fournie par l'outil de MDM pour les terminaux enrôlés si le type d'enrôlement le permet. Pour les terminaux non enrôlés dans l'outil de MDM, cette information de consommation de données peut éventuellement être disponible du côté des infrastructures réseau (par ex. l'outil de portail d'accès).

9.3. Gestion des productions numériques

Les productions numériques correspondent aux contenus créés par les élèves ou les enseignants et nécessaires à l'accomplissement des activités scolaires.

9.3.1. Stockage de productions numériques

Les productions numériques peuvent être stockées, dans le respect des durées de conservation et le respect de la règlementation sur la protection des données :

- sur l'équipement mobile, au sein de l'espace mémoire interne ou sur une carte mémoire externe de type *SD ;*
  dans ce cas, en cas de panne, les productions situées sur le matériel ou la mémoire interne sont perdues si elles n'ont pas été synchronisées au préalable ;
  les productions sur une carte externe sont facilement échangeables d'un équipement mobile à l'autre sous réserve que la charte autorise à retirer la carte mémoire ;

- sur un serveur de stockage partagé attaché au réseau de l'établissement ; le serveur garantit la sécurité des productions ;
- sur des sites distants (ENT, espace nuage, site éditeur…) ;
  ces sites s'apprécient selon les niveaux de sécurité, de volumétrie et de disponibilité proposés.

Dans le cas d'utilisation des espaces de stockage partagés, les utilisateurs **DOIVENT** être informés sur l'intérêt et sur les impacts (confidentialité) du stockage des données sur ces espaces.[20]

Dans le cas de sites dédiés, les contraintes de sécurité sont à étudier ainsi que la gestion des comptes utilisateurs.

Une surveillance et supervision de l'utilisation des capacités de stockage mises à disposition permet d'éviter les dysfonctionnements liés à des espaces saturés (émission d'alertes préventives, ajustement de la taille des espaces).

9.3.2. Sauvegarde / restauration et archivage des productions numériques

La sauvegarde, sur un support externe à l'équipement mobile, des productions stockées sur ce dernier permet en cas de problème sur celui-ci (unité de stockage défaillante, perte ou vol) d'assurer la récupération de ces données.

Une politique d'archivage est à définir si un besoin de ce type est identifié. Par exemple, si un élève doit pouvoir retrouver ses productions indépendamment de l'équipement mobile ou de ses changements de niveau. La fréquence d'archivage est alors à calibrer (trimestriel, annuel, pluriannuel) en adéquation avec le besoin remonté.

Par ailleurs ces mécanismes de sauvegarde / restauration et archivage étant très consommateurs en réseau, les fréquences et périodes de traitement sont à mettre en perspective des possibilités réseaux (bande passante) et des consommations attendues durant les heures de disponibilité des différents services.

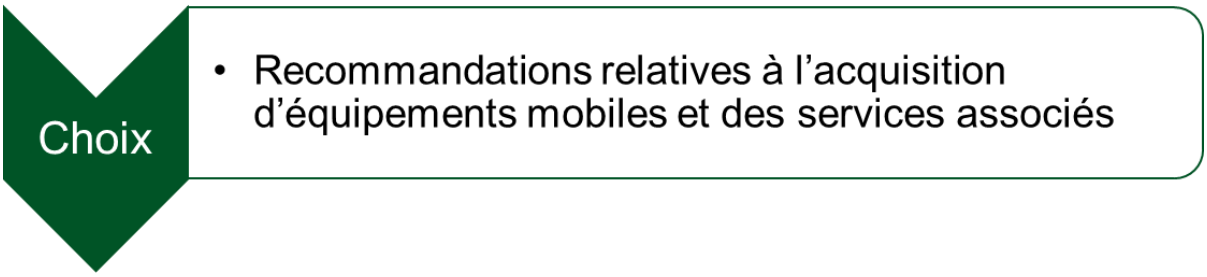
En outre, le délai légal de conservation au terme duquel une purge des données est nécessaire est à prendre à compte lors de la définition des mécanismes de sauvegarde / restauration et archivage.

9.3.3. Synchronisation des données

Certaines applications mobiles permettent de gérer un fonctionnement en mode déconnecté (c'est-à-dire sans avoir besoin d'un accès permanent à du contenu distant).

Ceci implique néanmoins la possibilité de synchroniser les données depuis l'équipement mobile et/ou vers l'équipement mobile en mode connecté (c'est-à-dire lorsque la connexion Wi-Fi est active). Les données échangées circulent entre l'équipement mobile et des sites dédiés, que ce soit des espaces de type nuage, un site éditeur, des serveurs internes.

[20] À consulter CARINE version 1.0 (http://eduscol.education.fr/carine), chapitre 3.4.5, page 74.


Choix
• Recommandations relatives à l'acquisition d'équipements mobiles et des services associés

10. Recommandations : introduction

Les chapitres 11 à 19 ci-après proposent des recommandations dont le but est d'aider les porteurs de projet à formuler leurs exigences pour le choix des équipements mobiles et des différents services nécessaires à la réussite de leur projet. Ces recommandations intéressent également les acteurs de la filière industrielle en ce sens qu'elles expriment des attentes pour le numérique éducatif.

Les prestataires de services évoqués dans ces chapitres peuvent être des acteurs académiques, de collectivités, ou des acteurs externes.

Le niveau d'exigence des recommandations formulées est exprimé suivant la terminologie RFC 2119[21], dont la traduction littérale des définitions est reprise comme suit :

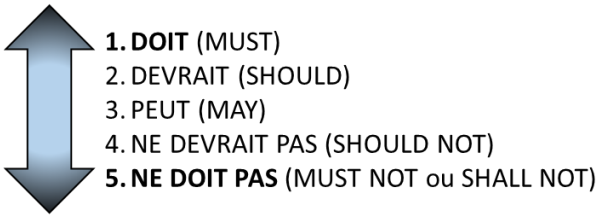


Illustration 19 : Niveau d'exigence des recommandations

1. **DOIT** : Ce terme signifie que la définition est une exigence absolue de la spécification.
2. **DEVRAIT** : Ce mot signifie qu'il peut exister des raisons valables dans des circonstances particulières pour ignorer un élément précis, mais toutes les implications doivent être comprises et soigneusement pesées avant de choisir une voie différente.
3. **PEUT** : Ce mot signifie que l'élément est vraiment facultatif.
4. **NE DEVRAIT PAS** : Cette phrase signifie qu'il peut exister des raisons valables dans des circonstances particulières où un comportement particulier est acceptable ou même utile, mais toutes ses implications devraient être comprises et le cas soigneusement pesé avant de mettre en œuvre un comportement décrit avec cette notation.
5. **NE DOIT PAS** : Cette phrase signifie que la définition est une interdiction absolue de la spécification.

Le Tableau 4 ci-après indique, pour chacun des domaines de l'architecture de référence, le chapitre de recommandations correspondant et/ou le chapitre où ses fonctions ont été décrites.

Domaine	Fonctions	Description au chapitre	Recommandations au chapitre
Services socle des équipements mobiles	Notification. Stockage Local. Services d'accès réseau et connectivité. Gestion des contacts. Système d'exploitation. Repérage spatio-temporel. Capture Multimédia. Gestion des environnements.	Chapitre 7.1 Caractéristiques et fonctionnalités d'un équipement mobile	Chapitre 11 Critères de choix d'un équipement mobile

[21] https://www.ietf.org/rfc/rfc2119.txt

Domaine	Fonctions	Description au chapitre	Recommandations au chapitre
Gestion des équipements mobiles	Gestion d'inventaire des équipements mobiles et des accessoires. Sauvegarde et restauration des équipements mobiles. Configuration de l'équipement mobile. Monitorage / compte rendu / statistiques des équipements mobiles. Application de la mise à jour des systèmes d'exploitation. Application des politiques de sécurité. Gestion des profils utilisateurs.	Chapitre 7.2 Gestion des équipements mobiles	Chapitre 12 Gestion des équipements mobiles (communément appelée MDM)
Distribution des applications mobiles	Gestion d'inventaire des applications mobiles. Monitorage / compte rendu / statistiques des applications distribuées. Association ressource / profil EM et/ou profil utilisateur. Store / portail d'accès aux ressources.	Chapitre 8.2 Distribution des applications mobiles	Chapitre 13 Distribution des applications mobiles (communément appelée MAM)
Services de gestion des productions numériques	Stockage des productions numériques. Sauvegarde / restauration et archivage des productions numériques ; Synchronisation des données.	Chapitre 9.3 Gestion des productions numériques	Chapitre 16 Gestion des productions numériques (communément appelée *MCM*)
Services de sécurité	Authentification. Autorisation. Définition des politiques de sécurité. Détection du non-respect des politiques de sécurité. Propagation des identités. Gestion des annuaires.	Chapitre 7.3 Sécurité de l'équipement mobile	Chapitre 14 Sécurité
Services d'infrastructure pour l'établissement	Gestion des systèmes informatiques (infogérance et serveurs) et composants réseaux. Services réseau. Monitorage / compte rendu / statistiques de l'infrastructure.	Chapitre 9.2 Services d'infrastructure pour l'établissement	Chapitre 15 Services d'infrastructure pour l'établissement
Services fonctionnels	Services de communication et de collaboration. Services informationnels et documentaires. Services de production pédagogique et éducative. Services d'accompagnement de la vie de l'élève. Services de gestion de classe.	Chapitre 8.1.1 Classement des services fonctionnels	Chapitre 17 Services fonctionnels de gestion de classe
Gestion des cycles de vie	Gestion du cycle de vie des équipements mobiles et accessoires.	Chapitre 7.7 Gestion du cycle de vie des équipements mobiles et des accessoires	
Gestion des cycles de vie	Gestion du cycle de vie des ressources numériques.	Chapitre 8.4 Gestion du cycle de vie des ressources numériques	
Support	Support matériel	Chapitre 0 . Support matériel	Chapitre 11.3 Support matériel
Support	Support logiciel	Chapitre 8.3 Support logiciel	Chapitre 18 Support logiciel

Tableau 4 : Vue d'ensemble de l'architecture – référence aux chapitres de description et recommandations

Le schéma présenté en Illustration 20 reprend ces mêmes informations sous forme graphique ; les chapitres de recommandation sont indiqués sur fond vert, les chapitres de description sur fond orange

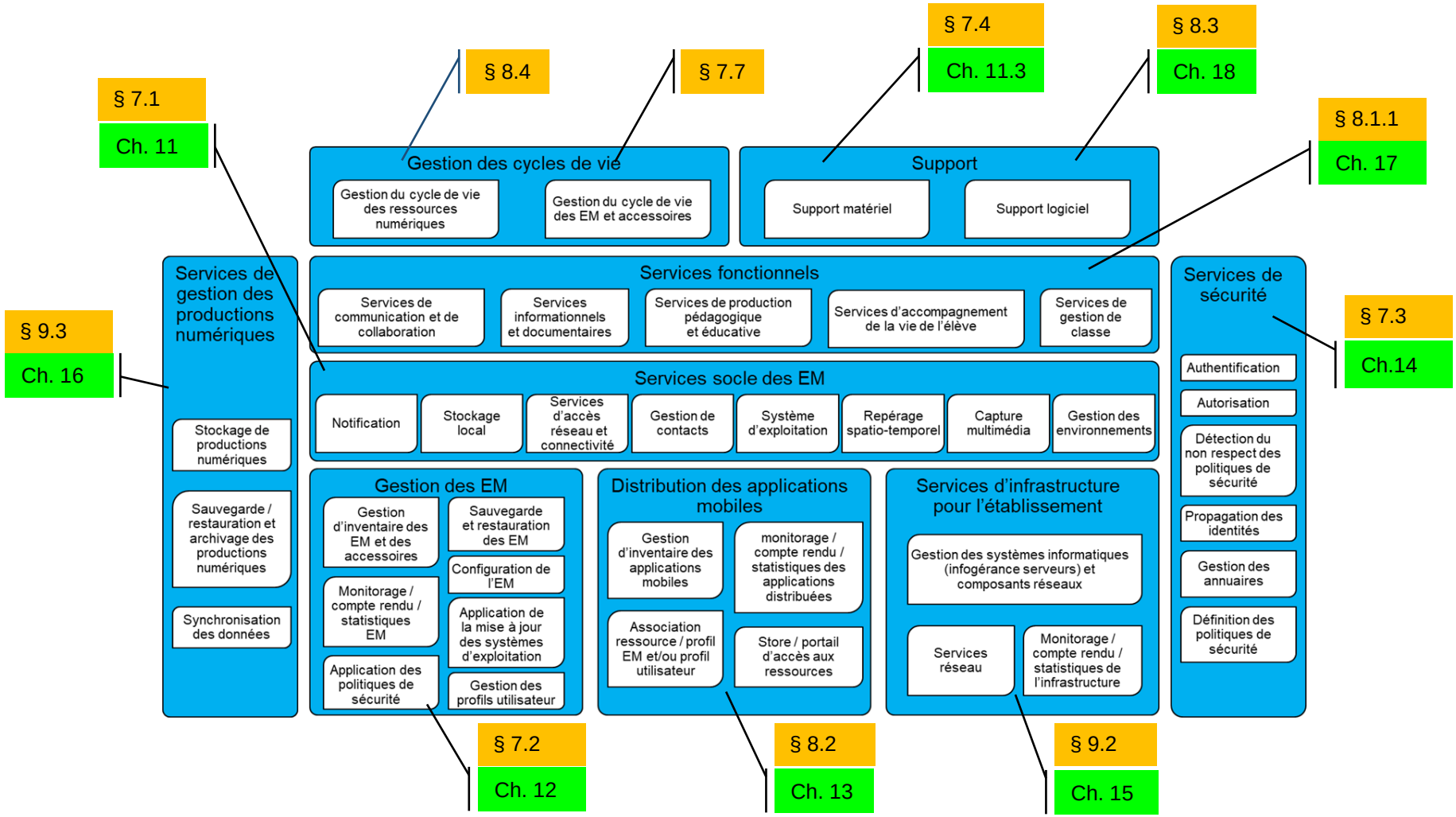


Illustration 20: Vue d'ensemble de l'architecture – référence aux chapitres de description et recommandations

11. Critères de choix d'un équipement mobile

Le choix de l'équipement mobile est un point essentiel dans l'équipement numérique des établissements et des écoles. En effet l'équipement mobile vient souvent accompagné d'un écosystème dans lequel il s'insère : outil de gestion matériel, outil de gestion logiciel, processus d'acquisition d'applications, sécurité des informations et protection des données à caractère personnel. Le support matériel et les différentes étapes de préparation d'un équipement mobile sont également des points importants dans le choix d'un équipement et des prestations associées.

Ce chapitre est destiné :

- aux parties prenantes dans l'acquisition d'EIM ou des classes mobiles (collectivités, académies) ou de terminaux BYOD (responsables des élèves ou autres) qui y trouveront des recommandations pour les guider dans leur choix ;
- aux fournisseurs de ressources qui seront intéressés de connaitre les recommandations importantes qui peuvent influer sur leur développement d'applications (taille d'écran, système d'exploitation…).

11.1. Caractéristiques et fonctionnalités

11.1.1. Caractéristiques

L'équipement mobile doit respecter un ensemble de caractéristiques et recommandations pour garantir un usage pertinent en établissement ou en école.

Ainsi la taille de l'écran **DEVRAIT** être supérieure à 9 pouces. Une taille inférieure à 9 pouces pénalise fortement les possibilités de lecture et de production de contenus. Des caractéristiques complémentaires (résolution, luminosité, angles de vision, contraste, résistif ou capacitif, tactile ou non, multipoints…) viennent compléter le choix de l'écran.

Par ailleurs, l'encombrement total de l'équipement mobile **DEVRAIT** respecter le format maximal 24x36 cm afin qu'il puisse être rangé dans un cartable, puisque l'utilisateur peut avoir besoin de le transporter en dehors de l'établissement. Pour les mêmes raisons, l'équipement mobile **NE DEVRAIT PAS** dépasser 1,2 kg hors accessoires.

Les élèves et les enseignants ont besoin de services de connectivité pour réaliser des opérations fréquentes : installation ou mise à jour *OTA* (*Over The Air*) d'applications ; lecture de contenu distant, production de contenu sur des serveurs distants, association d'accessoires sans fil… L'équipement mobile **DOIT** donc offrir les services de connectivité suivants : Wi-Fi 802.11, Bluetooth (minimum 3.0).

Une recommandation complémentaire sur la connectivité concerne la connexion au réseau de l'établissement : l'équipement mobile **DOIT** pouvoir se connecter de manière sécurisée au réseau Wi-Fi de l'établissement.

L'équipement mobile **PEUT** offrir la possibilité de diffuser des flux vidéo sur un vidéoprojecteur ou un écran externe.

Les salles de classe n'étant pas équipées pour permettre un chargement de tous les équipements mobiles des élèves, l'équipement mobile **DEVRAIT** offrir une autonomie suffisante pour une journée de cours, soit 8 heures, sans avoir besoin d'être rechargé. Dans le cas d'une classe mobile, le rechargement électrique des équipements mobiles s'opère à travers le conteneur.

Cela signifie que les équipements mobiles devraient être rechargés quotidiennement :

- à la maison pour les établissements ou écoles dont les élèves emportent les EIM à domicile ;

- en établissement ou à l'école pour les cas contraires, dans un local équipé prévu et aménagé à cet effet.

Les équipements mobiles possèdent une mémoire interne limitée, sur laquelle il faut déduire la place occupée par le système d'exploitation. L'équipement mobile **PEUT** accueillir une mémoire externe de type carte *micro SD* par exemple pour étendre ses capacités mémoire. Le faible coût des mémoires externes peut aider à contrer un remplissage précoce de la mémoire de l'équipement mobile.

Que la mémoire soit uniquement interne ou bien étendue par une carte externe, la mémoire disponible **DEVRAIT** être au minimum de 32 Go[22] pour l'utilisateur (hors système d'exploitation et applications). Cet espace est utilisé pour l'installation d'applications, de mises à jour du système et la production de contenus.

L'élève et l'enseignant partageront beaucoup d'applications (outil de gestion de classes, manuels…) qui nécessitent d'avoir un écosystème commun. Il est par ailleurs plus simple de communiquer et d'échanger du contenu sur un même écosystème. C'est pourquoi le système d'exploitation et les capacités de connexion des équipements mobiles des enseignants **NE DEVRAIENT PAS** être différentes de celles des équipements mobiles des élèves (la version du système d'exploitation, la taille d'écran, la puissance et la capacité mémoire peuvent cependant différer).

Afin de connecter un accessoire permettant d'écouter et produire du contenu audio, l'équipement mobile **DOIT** disposer d'une prise sortie audio et d'une entrée microphone, ou de Bluetooth (minimum 3.0). L'équipement mobile **PEUT** proposer les deux solutions. Ces caractéristiques sont particulièrement utiles dans certaines disciplines - langues vivantes, éducation musicale… - ainsi que pour des dispositifs de compensation de handicap.

Pour pouvoir répondre à certains besoins de production photo ou vidéo (dans des disciplines comme l'EPS par exemple) l'équipement mobile **DOIT** disposer d'au moins une caméra. Le nombre de caméras et leur qualité **DOIVENT** être adaptés aux usages. Pour une visioconférence, l'usage de la lecture labiale par les malentendants dépend de la qualité de l'image capturée (ainsi que de son transport sur le réseau et de sa restitution selon la qualité du logiciel et de l'écran).

L'équipement mobile **PEUT** disposer de connecteurs physiques permettant d'associer des périphériques (stockage externes, accessoires…).

Les fonctions d'accessibilité disponibles sont également à considérer dans le choix de l'équipement mobile, en particulier celles offertes nativement par le système d'exploitation.

11.1.2. Accessoires

Les équipements mobiles sont des produits exposés à des casses - d'écran notamment – et manipulés par des enfants. C'est pourquoi une housse ou une coque de protection **DOIT** être associée à l'équipement mobile si celui-ci n'est pas renforcé pour limiter les dommages.

Un film protecteur **PEUT** être associé à l'équipement mobile.

La housse de protection **DEVRAIT** permettre de mettre l'équipement mobile en position verticale ou inclinée et pas uniquement à plat, ce qui rendra le visionnage des supports plus aisé.

Les équipements mobiles possèdent tous des claviers virtuels, dont l'utilisation n'est pas conforme pour une production de contenu de masse. Or les élèves et les enseignants ont besoin de produire du contenu, aussi rapidement que possible et sans que l'outil utilisé soit une gêne. Ainsi un clavier physique compatible avec l'équipement mobile **DEVRAIT** être associé à l'équipement mobile.

[22] Attention : changement par rapport à la version 1 de CARMO où la valeur indiquée était de 16 Go.

En tout état de cause, aucune fonctionnalité d'authentification de la dynamique de frappe au clavier **NE DOIT** être déployée.

Le clavier virtuel présente cependant l'intérêt de pouvoir s'adapter au contexte d'usage de l'appareil, et offre une solution au problème des caractères spécifiques.

Points d'attention concernant les claviers physiques :

- les claviers intégrés à la housse de protection sont susceptibles de dégrader l'usage mobile de l'équipement (obligation d'emmener systématiquement le clavier) ;
- certains équipements font reposer le clavier directement sur la vitre de l'équipement mobile lors du rangement et sont susceptibles d'endommager cette dernière voire de la casser ;
- les claviers sans fil (par ex : Bluetooth) constituent un accessoire supplémentaire à recharger, et peuvent poser des problèmes d'appairage avec l'équipement mobile.

Des claviers spécifiques **DOIVENT** être proposés pour des personnes en situation de handicap (plage braille, claviers alternatifs, claviers à suivi oculaire, claviers virtuels…).

L'équipement mobile doit répondre à de nombreuses situations et permettre des usages variés. Des accessoires **PEUVENT** être associés à l'équipement mobile (exemples : stylet de pointage, stylet à pointe fine permettant d'écrire en posant la main, sondes techniques…), selon les usages pédagogiques attendus dans l'école ou l'établissement, ou des besoins particuliers (exemple : compensation de handicap).

Plusieurs disciplines ou situations (langues vivantes, éducation musicale, sortie scolaire, baladodiffusion, certains cas de handicap visuel) nécessitent l'utilisation de casques ou d'écouteurs. Un dispositif d'écoute individuel (casque, écouteurs) **DOIT** être associé à l'équipement mobile.

Les accessoires sélectionnés afin de compléter les équipements mobiles **DOIVENT** être adaptés afin de ne pas dégrader l'usage. Par exemple, veiller à ce que la housse de protection n'obstrue pas la caméra, le micro, les haut-parleurs, les prises de branchement, les boutons…

11.2. Étapes de préparation et de livraison d'un équipement mobile

Dans le cas des projets BYOD, certaines des opérations de préparation et de livraison qui sont valables pour les équipements mobiles peuvent ne pas s'appliquer.

Contractuellement, le prestataire **DOIT** être tenu d'assurer la sécurité et la confidentialité des données à caractère personnel auxquelles il pourrait avoir accès dans le cadre de ses prestations.

11.2.1. Liste des services attendus (fonctionnalités)

Avant d'être mis à disposition des utilisateurs les équipements mobiles doivent suivre plusieurs étapes préalables.

Ces étapes pourront être prises en charge par un prestataire, qui devra réaliser plusieurs opérations et manipulations sur les équipements mobiles. Dans le reste du chapitre le prestataire peut être soit externe soit la collectivité.

11.2.1.1. Assemblage de l'équipement mobile

Cette opération consiste à ajouter certains accessoires à l'équipement mobile. Il s'agit par exemple de placer la housse de protection sur l'équipement mobile si une housse a été choisie et acquise. Il en va de même pour un film de protection de l'écran, ou une carte mémoire additionnelle. Enfin il aura peut-être été décidé d'étiqueter l'équipement mobile dès la phase d'assemblage afin de garantir un suivi et une traçabilité de l'équipement mobile.

Ainsi, si une housse a été choisie, le prestataire **DOIT** placer la housse de protection. Étant donné le volume d'équipement mobile à assembler ce travail ne peut être opéré en établissement.

De la même manière le prestataire **DOIT** placer le film de protection de l'écran si un film a été choisi et acquis et le prestataire **DOIT** insérer - et formater selon les cas - la carte mémoire additionnelle si une carte a été choisie et acquise.

Remarque : il est important dans le calendrier que le prestataire ait en sa possession suffisamment tôt ces accessoires afin de les assembler.

Enfin le prestataire **DEVRAIT** étiqueter les équipements mobiles pour garantir une bonne gestion de l'inventaire ou du suivi des réparations.

11.2.1.2. Installation de l'image

Lorsque l'équipement mobile arrive chez le prestataire, le système d'exploitation n'est pas nécessairement à niveau concernant les mises à jour et différents correctifs de sécurité, il convient d'installer ces éventuels mises à jour et correctifs.

Par ailleurs plusieurs applications sont à installer lors de cette étape :

- l'agent *MDM* prend souvent la forme d'une application, qu'il convient de préinstaller ;
- l'académie, l'école ou l'établissement ayant peut-être prévu un socle d'applications commun à tous les utilisateurs, ces applications **PEUVENT** être installées lors de cette phase.

Certains paramétrages sont nécessaires pour une utilisation « clé en main » de l'utilisateur : configuration Wi-Fi de l'école ou de l'établissement, paramétrage des éléments de sécurité.

Le prestataire **DOIT** automatiser toutes ces manipulations (installation des dernières mises à jour, du *master* établissement, de l'agent *MDM*, configuration du Wi-Fi établissement, application des règles de sécurité).

11.2.1.3. Activation de l'équipement mobile

Le prestataire **DOIT** pouvoir récupérer les données du *MxM* (*profils* utilisateurs, applications) et les appliquer aux équipements mobiles.

11.2.1.4. Finalisation

Le prestataire **DOIT** pouvoir lors de la préparation initiale de l'équipement mobile, y installer du contenu (audio, vidéo, PDF…) et lui associer le matériel Bluetooth (clavier ou casque par exemple).

11.2.1.5. Expédition

Un système de livraison des terminaux (nouveaux équipements mobiles ou suite à une réparation) **DOIT** être mis en place.

11.2.2. Impact organisationnel (rôles et acteurs)

La fourniture des accessoires a un impact organisationnel différent selon le mode choisi :

- si les accessoires sont commandés par le prestataire, ce dernier a la charge de l'acquisition et est complétement autonome pour la phase d'assemblage ;
- si les accessoires ne sont pas commandés pas le prestataire, le porteur de projet aura la charge de coordonner les différents prestataires et devra s'assurer que les accessoires parviennent au prestataire responsable de l'assemblage conformément au planning.

La mise à disposition des équipements mobiles aura également des impacts différents selon le mode choisi :

- la distribution peut être à la charge du prestataire responsable de la préparation : dans ce cas le prestataire vient dans l'école ou l'établissement, et gère la mise à disposition aux élèves et aux enseignants ; cette solution est presque transparente pour l'école ou l'établissement, qui a seulement à fournir un espace au prestataire pour lui permettre réaliser l'opération ;
- la distribution peut être assurée par l'école ou l'établissement ; dans ce cas une personne devra porter un rôle de relais pour assurer la réception des équipements mobiles et la mise à disposition auprès des élèves et des enseignants ; il faut dans ce cas prévoir un espace de stockage temporaire entre la livraison et la distribution. Cette distribution peut être faite pendant la remise des livres.

Quel que soit le mode choisi, une réunion devra être organisée pour les parents, les élèves et les enseignants. Cette réunion est l'occasion d'informer et de présenter l'équipement mobile, ses caractéristiques, son utilisation, l'accès aux ressources, son entretien. Elle est aussi l'occasion d'informer les usagers de leurs droits relatifs à leurs données personnelles.

La charte utilisateur reprenant les règles à suivre **DOIT** être remise ou rappelée aux utilisateurs. Elle **PEUT** être distribuée lors de la mise à disposition de l'équipement mobile. Elle **PEUT** être sous forme numérique préchargée sur l'équipement mobile.

11.2.3. Modalités opérationnelles

Pour mener à bien les étapes de préparation des équipements mobiles, le prestataire devra pouvoir disposer des informations suivantes :

- les codes d'inventaire à apposer sur les étiquettes si utilisation de ce mécanisme de traçage ;
- les applications à déployer sur les groupes d'équipements mobiles (il peut par exemple y avoir un *master* pour les élèves et un autre pour les enseignants) ;
- les données (contenu audio, manuels PDF…) à déployer sur les équipements mobiles ;
- les informations pour se connecter à l'outil de gestion de flotte.

Toutes ces informations devront être échangées entre les parties sous un format à définir entre elles.

Par ailleurs le prestataire responsable des étapes de préparation devra avoir en sa possession les accessoires : les cartes mémoires additionnelles, les housses de protection, et les films de protection. Ces accessoires doivent lui parvenir dans un délai à définir si le prestataire n'est pas responsable de l'acquisition des accessoires.

Le prestataire pourra réaliser un certain nombre de préparations d'équipements mobiles dans un temps imparti. Cela permettra de définir une stratégie de dotation pour l'école ou l'établissement, selon le temps de préparation et le nombre total d'équipements mobiles à préparer :

- soit le délai est suffisant pour préparer tous les équipements mobiles avant la rentrée ;

- soit il faudra définir un étalement dans le temps des dotations, par vagues (par niveau par exemple).

Les engagements du prestataire **DOIVENT** être formalisés par le biais d'un contrat, sur par exemple les garanties de confidentialité quand l'activation de l'équipement mobile nécessite des données sur les utilisateurs.

11.3. Support matériel

La gestion des pannes matérielles impose un support répondant aux problématiques des utilisateurs et des gestionnaires du matériel. Ce support propose des services et s'adosse à une organisation à mettre en œuvre.

11.3.1. Liste des services attendus (fonctionnalités)

D'une manière générale, une prestation de support matériel **DOIT** être proposée, elle est incontournable dans la vie d'un équipement mobile pour gérer les différentes situations (casse ou panne principalement).

L'image de l'équipement mobile (applications + données + paramètres de configuration) **DOIT** être sauvegardée pour remonter un équipement mobile à l'identique (opération de restauration).

Le prestataire **DOIT** fournir un état périodique des interventions de support qu'il réalise. Des indicateurs **DOIVENT** être définis dans ce sens (temps de résolution d'incident, commentaire de satisfaction utilisateur final…)

11.3.2. Impact organisationnel (rôles et acteurs)

Le changement organisationnel dépend de l'organisation proposée et des acteurs impliqués.

Si le support matériel est intégralement pris en charge par un prestataire externe, ce dernier est l'unique interlocuteur avec l'élève (assisté par un adulte) ou l'enseignant. L'établissement ou l'école n'intervient donc pas dans cet échange.

Cependant, on **PEUT** envisager que l'établissement ou l'école possède un premier niveau de diagnostic de la panne, pour éviter de solliciter inutilement le support téléphonique.

Quelle que soit la solution choisie, l'établissement ou l'école **DOIT** prévoir plusieurs équipements mobiles de remplacement. En effet, même si une réparation d'équipements mobiles peut être rapide, le processus d'envoi-réparation-retour peut prendre plusieurs jours. L'élève, surtout dans le second degré, ne peut pas se passer d'outil numérique aussi longtemps car il risque de ne pas avoir les mêmes moyens que les autres élèves. Des chargeurs supplémentaires **DOIVENT** également être disponibles pour les équipements mobiles qui ne sont pas rechargés. Ces chargeurs supplémentaires peuvent être remplacés par des batteries qui seraient prêtées aux utilisateurs dont les équipements ne sont pas chargés.

Si l'indisponibilité est de l'ordre de la journée, on peut admettre que l'élève suivra les cours aux côtés d'un autre élève. En revanche, pour une indisponibilité plus longue ou dans le cas d'un enseignant, l'établissement ou l'école **DOIT** pouvoir proposer un équipement mobile de remplacement. Cet équipement aura alors les ressources de base de l'établissement ou de l'école, mais ne sera pas nécessairement personnalisé comme il le serait dans le cas d'une attribution individuelle classique (cf. les phases de préparation de l'équipement mobile). Selon les possibilités de la solution, l'équipement mobile de remplacement **PEUT** être automatiquement configuré en fonction de l'utilisateur par récupération des paramètres et applications de l'utilisateur.

11.3.3. Modalités opérationnelles

En cas de panne, les élèves et les enseignants **DOIVENT** se voir proposer un numéro de téléphone et une plateforme d'assistance en ligne. Le support matériel **DOIT** être accessible sur une plage horaire définie et communiquée à l'ensemble des appelants potentiels. Les techniciens de cette assistance téléphonique guident alors l'utilisateur sur les démarches à entreprendre. Un contrôle des appelants **PEUT** exister afin d'éviter les appels sans rapport avec le support.

Si l'assistance décide que l'équipement mobile doit être envoyé en réparation, plusieurs formules sont possibles, notamment :

- l'établissement ou l'école sert de relais et d'interface entre l'utilisateur et le réparateur ;
- un transporteur est chargé de passer enlever le colis au domicile de l'utilisateur.

Les conditions de prise en charge **DOIVENT** être précisées au moment de la remise de l'équipement (cf. §21.2.6 « Élaboration des conventions & chartes et protection des données à caractère personnel»). Les dispositions applicables pendant les vacances scolaires **DOIVENT** être mentionnées.

Des colis de retour prêts à l'emploi **PEUVENT** être proposés par le prestataire du support.

Le suivi **DOIT** être assuré avec par exemple un numéro d'incident fourni à l'utilisateur ou l'établissement ou l'école.

Un temps de prise en charge et de durée maximum de réparation **DOIT** être défini avec le prestataire en charge de la réparation.

La sauvegarde des données pédagogiques **DEVRAIT** être automatique et transparente pour l'utilisateur. En revanche la sauvegarde des données privées est à l'initiative de l'utilisateur, elle se fera par exemple en sauvegardant les informations sur une clé USB ou un disque externe.

Une procédure de restauration **DOIT** être mise en place pour les données pédagogiques. La restauration des données privées est à l'initiative et à la charge de l'utilisateur.

De manière à assurer une continuité de service en cas d'incident, le projet **DOIT** prévoir des équipements mobiles de rechange à proposer aux élèves et enseignants pour compenser une indisponibilité de longue durée de leurs équipements mobiles, en particulier dans le cas des projets BYOD. Le projet **DEVRAIT** prévoir dans ce cas des équipements avec les systèmes d'exploitation les plus répandus afin d'éviter des problèmes d'incompatibilité des contenus et des applications. Le nombre d'équipements mobiles de réserve sera à définir en fonction du nombre d'équipements mobiles du projet ; le ratio **NE DEVRAIT PAS** être inférieur à 2 %. Il est recommandé de limiter dans le temps la durée des remplacements. Cette recommandation peut se traduire par une clause spécifique dans la charte d'usage lors de la remise de l'équipement de remplacement.

12. Gestion des équipements mobiles (communément appelée MDM)

Cette partie concerne les porteurs de projet qui doivent prendre en charge la mise en œuvre d'un outil de gestion des équipements (fonction *MDM*).

12.1. Liste des services attendus (fonctionnalités)

L'outil de gestion des équipements mobiles doit répondre à un certain nombre de fonctionnalités décrites ci-après sous forme de recommandations.

- Les équipements mobiles déployés **DOIVENT** pouvoir être inscrits grâce à la fonction MDM, qui peut ainsi proposer une vision unique du parc géré.
- La fonction MDM **DEVRAIT** pouvoir contrôler l'accès au paramétrage de l'équipement mobile. Cela permet d'empêcher les mauvaises manipulations des utilisateurs (volontaires ou non).
- La fonction MDM **DEVRAIT** permettre d'interdire l'accès à certaines applications (par exemple le store).
- La fonction MDM **DEVRAIT** pouvoir envoyer des notifications aux équipements mobiles. Les notifications sur les équipements mobiles sont un moyen rapide et efficace pour communiquer avec tout ou partie des équipements mobiles sans avoir à recourir à des envois de mails.
- La fonction MDM **DOIT** pouvoir proposer la création de groupes d'équipements mobiles à usages différenciés : par niveau, discipline, profils utilisateurs…
  - Ces usages différenciés incluent des politiques de sécurité différentes. Ainsi un enseignant pourra avoir accès aux magasins d'applications, alors que cela serait interdit à l'élève.
  - Ils permettent la mise en place de configurations spécifiques adaptées à certains usages ou situations (notamment de handicap).
- La fonction MDM **DOIT** pouvoir contrôler la façon dont les équipements mobiles sont sécurisés. Cette recommandation permet de garantir le respect des politiques de sécurité et les éventuels contournements.
- Les ROM (systèmes d'exploitation) en cours d'utilisation sur les équipements mobiles **DOIVENT** être surveillées.
- La fonction MDM **DOIT** pouvoir suivre le rythme des mises à jour des systèmes d'exploitation des équipements mobiles.
- La mise à jour des correctifs de sécurité du système d'exploitation **NE DOIT PAS** être automatique. Les changements peuvent rendre inutilisables plusieurs applications en attendant qu'elles soient mises en conformité. Ce délai ne doit pas empêcher un usager de recourir normalement à l'équipement mobile qu'il utilise.
- Une fonction administrative de sécurité **PEUT** être proposée pour bloquer un équipement mobile.
- La fonction MDM **DOIT** pouvoir auditer les équipements mobiles. Le projet **DOIT** préciser les fonctionnalités précises attendues de ces audits.
- Les administrateurs de la fonction MDM **PEUVENT** utiliser ses fonctionnalités MDM pour réaliser des opérations associées à la sécurité sur les équipements mobiles (telles que : effacement ou changement mot de passe, verrouillage équipement mobile).
- La fonction MDM **DOIT** offrir un support en français.
- Pour prévenir tout acte de malveillance, l'accès aux fonctionnalités et aux données de la fonction de MDM **DOIT** être sécurisé en conformité avec les recommandations en matière de sécurité de l'ANSSI et de la Cnil.

- La mise en place de la fonction MDM **NE DOIT PAS** entrainer un blocage des applications ou des configurations destinées aux élèves en situation de handicap.
- La compatibilité équipements mobiles / fonction MDM **DOIT** être vérifiée afin de bénéficier de la totalité des fonctionnalités de l'outil de gestion de flotte, en particulier :
  - compatibilité entre la version du système d'exploitation ou les personnalisations du constructeur avec les fonctions du MDM ;
  - capacité du MDM à intégrer les services proposés avec les systèmes d'exploitation.
- L'adresse MAC[23] **NE DEVRAIT PAS** être utilisée par la fonction de MDM comme identifiant unique de l'équipement mobile (risque d'usurpation).

12.2. Impact organisationnel (rôles et acteurs)

Différents rôles et acteurs sont nécessaires au fonctionnement d'une solution de gestion de flotte :

- l'exploitant qui a en charge de gérer la plateforme technique (paramétrage, maintenance et exploitation) ;
- l'administrateur qui a en charge :
  - l'association entre les EIM et les utilisateurs,
  - le respect des politiques de sécurité et de la conformité des règles mises en place ;

  Il peut s'agir d'un administrateur central si la solution est multi-établissements ou d'un administrateur local (ex référent dans un établissement et école).

Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** s'assurer que les traitements de données mis en œuvre s'effectuent en conformité avec les dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018. Voir au § 21.2.621.2.6.

12.3. Modalités opérationnelles

Les EIM sont associés à des utilisateurs. Dans ce cadre, la fonction MDM **DOIT** pouvoir s'interfacer avec le référentiel d'identité dans le respect des dispositions relatives à la protection des données et en particulier des principes de finalité, de proportionnalité et de minimisation.

La fonction MDM **DOIT** pouvoir gérer l'ensemble des équipements mobiles de son périmètre, sachant qu'une même solution pourra gérer plusieurs établissements et/ou écoles. La fonction MDM **DOIT** en conséquence être capable de cloisonner de manière totalement étanche la gestion des équipements mobiles par structure organisationnelle.

Que la fonction MDM soit infogérée ou non certaines recommandations sont incontournables :

- une plage de service et de maintenance **DOIT** être définie ;
- la disponibilité attendue durant la plage de service **DOIT** être définie ;
- la solution technique retenue pour la fonction MDM **DOIT** être en phase avec la stratégie de déploiement et donc être évolutive pour prévoir la charge ;
- la solution technique retenue pour la fonction MDM **DOIT** permettre la délégation de rôles aux établissements et écoles.

La fonction MDM **DOIT** être à même d'interagir techniquement avec ses partenaires dans le respect des dispositions relatives à la protection des données et en particulier des principes de finalité, de proportionnalité et de minimisation des données :

- le référentiel d'identité (annuaire LDAP, Active Directory, SQL…) : la fonction MDM **DOIT** pouvoir collecter automatiquement les informations ou **DOIT** être mise à jour par réplication ;

[23] Voir glossaire : Adresse MAC – MAC address

- le système du partenaire responsable de la préparation des équipements mobiles : la fonction MDM **DEVRAIT** pouvoir mettre à disposition les informations nécessaires (paramètres, applications à préinstaller, politiques de sécurité, profil…) ;
- la solution de gestion de parc établissement : les modalités sont précisées dans le référentiel S2I2E - CARINE intégrant la mobilité.

13. Distribution des applications mobiles (communément appelée MAM)

Cette partie concerne les porteurs de projet qui doivent commander l'outil portant les fonctions de distribution des applications mobiles associé au choix de l'équipement mobile (*MAM*).

13.1. Liste des services attendus (fonctionnalités)

Les fonctionnalités attendues pour les services de MAM sont décrites ci-après sous forme de recommandations.

- La fonction MAM **DOIT** permettre d'encadrer l'installation, la désinstallation et la mise à jour des applications.
- L'installation et la mise à jour d'applications **DOIT** pouvoir être faite par *OTA (Over The Air)*. La fonction MAM **DEVRAIT** dans ce cas permettre une optimisation des flux sur l'infrastructure locale.
- L'installation et la mise à jour d'applications **PEUT** être réalisée en mode poussé (push) silencieux ou en mode tiré (pull) en fonction des choix du projet. La fonction MAM **DOIT** pouvoir réaliser la modalité choisie.
- La fonction MAM **DOIT** pouvoir affecter une application au niveau établissement ou école, au niveau groupe ou au niveau individuel.
- La fonction MAM **DEVRAIT** être informée des commandes passées sur les dispositifs d'acquisition d'applications.
- La fonction MAM **DOIT** pouvoir suivre le rythme des mises à jour des systèmes d'exploitation des équipements mobiles.
- La fonction MAM **DOIT** offrir un support en français.
- Pour prévenir tout acte de malveillance, l'accès aux fonctionnalités et aux données de la fonction MAM **DOIT** être sécurisé.

13.2. Impact organisationnel (rôles et acteurs)

L'organisation précise va dépendre du mode de fonctionnement de la plateforme d'acquisition mais d'une manière générale la répartition des rôles est la suivante :

- Les enseignants **DOIVENT** être impliqués dans la composition du portefeuille applicatif.
  - L'accès au store applicatif associé au système d'exploitation **DOIT** être autorisé pour les enseignants afin de maximiser la découverte de nouvelles applications.
- Les applications mobiles sont acquises sur la plateforme d'acquisition pour un certain volume de licences.
  - Les informations concernant le délai de mise à disposition d'une nouvelle application **DOIVENT** être partagées avec les utilisateurs afin qu'ils puissent anticiper leurs demandes.
  - Un processus organisationnel permettant de regrouper les demandes et de s'assurer qu'elles sont traitées dans des délais raisonnables par les administrateurs **DEVRAIT** être mis en œuvre.
- Le plus souvent, le MAM récupère auprès de la plateforme d'acquisition les binaires de l'application mobile ; il peut également n'enregistrer que l'adresse d'installation.
- Un responsable affectation associe depuis l'interface du MAM l'application à des groupes ou à des utilisateurs.

- Si l'affectation est réalisée dans un dispositif autre que le MAM alors les informations d'affectation **DOIVENT** être remontées dans le MAM

- Le MAM se charge de distribuer automatiquement les applications ou d'instancier leur téléchargement et leur installation à distance.

Par ailleurs, l'exploitant a en charge de gérer la plateforme technique (paramétrage, maintenance et exploitation).

Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** s'assurer que les traitements de données mis en œuvre s'effectuent en conformité avec les dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018 et notamment que ces traitements sont inscrits dans son registre (cf. § 21.2.6 « Élaboration des conventions & chartes et protection des données à caractère personnel »).

13.3. Modalités opérationnelles

Les EIM sont associés à des utilisateurs, la fonction MAM **DOIT** donc pouvoir s'interfacer avec le référentiel d'identité dans le respect des dispositions relatives à la protection des données et en particulier des principes de finalité, de proportionnalité et de minimisation des données.

La fonction MAM **DOIT** pouvoir gérer l'ensemble des équipements mobiles de son périmètre, sachant qu'une même solution pourra gérer plusieurs établissements et/ou écoles. La fonction MAM **DOIT** en conséquence être capable de cloisonner de manière totalement étanche la mise à disposition des ressources par structure organisationnelle.

La fonction MAM **DEVRAIT** s'intégrer fortement avec la fonction MDM. Il s'agit d'ailleurs souvent d'un même logiciel.

Que la fonction MAM soit infogérée ou non, certaines recommandations sont incontournables :

- une plage de service et de maintenance **DOIT** être définie ;
- la disponibilité attendue durant la plage de service **DOIT** être définie.

La fonction MAM **DOIT** être à même d'interagir techniquement avec la technologie du référentiel d'identité (annuaire LDAP, AD, SQL…).

La fonction MAM **DOIT** permettre la délégation de rôles aux établissements et écoles.

La fonction MAM **DEVRAIT** s'intégrer fortement avec la plateforme d'acquisition d'applications pour obtenir automatiquement les informations suivantes :

- le binaire de l'application à déployer ;
- le descriptif et les contraintes techniques pour connaitre dans le MAM les équipements mobiles compatibles avec l'application ;
- le nombre de licences.

La fonction MAM **DEVRAIT** s'appuyer sur la même gestion des groupes que le MDM pour éviter une administration complexe. La plupart des offres du marché offrent ces fonctions dans une même solution MxM.

14. Sécurité

Les acteurs d'un projet de déploiement d'équipements mobiles **DOIVENT** mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Le présent chapitre fournit des recommandations relatives à la sécurité. De son côté, la Cnil a également émis des recommandations et mesures minimales à mettre en œuvre pour assurer la sécurité des données. Ces mesures sont consultables sur son site web[24].

14.1. Risques et vulnérabilités

De nombreux éléments d'exposition aux risques sont à considérer :

- l'utilisateur, pour qui le contenu pour adulte ou les communications inappropriées sont une menace ; des mécanismes de protection (filtrage…) **DOIVENT** donc être mis en place dans le cadre scolaire[25]. Hors de ce cadre, il revient aux responsables légaux d'assurer le contrôle de ces accès ;
- l'équipement mobile, qui peut être perdu, volé ou utilisé frauduleusement ;
- le contenu et les données associées, qui sont vulnérables durant 3 moments clé :
  - quand la donnée est sur l'équipement mobile,
  - quand la donnée transite par le réseau,
  - quand la donnée est stockée sur un serveur distant et que l'utilisateur interagit avec la donnée au travers d'une application ;
- l'application, qui peut être contaminée par un virus, un ver, un logiciel espion ;
- la transaction, via une interception de communication de données entre l'équipement mobile et des serveurs distants ;
- l'infrastructure, qui peut faire l'objet d'une attaque de type déni de service (*DoS ou DDoS*).

14.2. Définition des politiques de sécurité

Un projet de déploiement d'équipements mobiles et de mise à disposition de ressources numériques induit un ensemble de risques (voir le chapitre 14.414.1 « Risques et vulnérabilités » sur ce point) dont il faut se prémunir au mieux.

Les objectifs de sécurité concernant les équipements mobiles **DOIVENT** être intégrés dans la politique de sécurité informatique de l'établissement.

Une politique de sécurité définit un ensemble d'actions qui permettront de maintenir le niveau de sécurité jugé acceptable par rapport aux risques identifiés et encourus. Cette politique de sécurité informatique fixe les objectifs de sécurité des systèmes informatiques mis en œuvre.

Ces objectifs de sécurité touchent les domaines suivants :

- l'information et les données, dont la protection et la confidentialité des données personnelles ;
- les systèmes d'exploitation ;
- les flux de communication ;
- les applications ;

[24] Guide de la sécurité des données personnelles de la Cnil : https://www.cnil.fr/fr/un-nouveau-guide-de-la-securite-des-donnees-personnelles
[25] Voir glossaire

- les infrastructures informatiques ;
- la sensibilisation des utilisateurs aux enjeux de sécurité ;
- la géolocalisation.

Sur chacun de ces domaines, il convient :

- de définir les règles à respecter, les procédures à suivre, d'installer des outils techniques associés ;
- de préciser les actions à entreprendre et identifier les points de contact en cas de détection d'une faille de sécurité, d'une intrusion dans le système ;
- de décrire les rôles et responsabilités des parties prenantes (les utilisateurs, élèves et enseignants, les responsables informatiques de la collectivité en charge de la gestion de tout ou partie du système des équipements mobiles et ressources numériques, les différents prestataires et les fournisseurs de solutions).

Pour élaborer cette politique de sécurité dans le contexte des équipements mobiles et des ressources numériques, il convient de veiller à prendre en considération les recommandations de l'ANSSI et de la Cnil dans ce domaine et de répondre aux questions suivantes :

- Comment contrôle-t-on l'accès à l'équipement mobile ?
- Quelles sont les règles à respecter sur la forme des identifiants / mots de passe d'accès (nature de l'identifiant, nombre et type de caractères du mot de passe) ?
- Quel est le référentiel d'identité qui doit être utilisé dans les phases d'authentification de l'utilisateur et d'autorisation d'accès à une ressource ?
- Comment l'équipement mobile accède-t-il au réseau Wi-Fi de l'établissement, de la collectivité ? Au moyen d'une authentification par certificat utilisateur, clé ou autre identifiant ?
- Comment contrôle-t-on l'intégrité du système d'exploitation de l'équipement mobile (débridage) ?
- Met-on en place une solution de protection contre les logiciels malveillants sur les équipements mobiles ?
- Autorise-t-on l'utilisateur à installer des ressources depuis les stores publics ?
- Est-ce que certaines des données stockées sur l'équipement mobile sont confidentielles ? Quels mécanismes de chiffrement applique-t-on ? Pour les données personnelles, quel processus d'effacement applique-t-on ?
- Doit-on mettre en œuvre, dans le respect des exigences légales, les traces des actions utilisateur ?
- En cas d'identification d'une faille de sécurité sur une application, un système d'exploitation d'un équipement mobile, y a-t-il une mise en quarantaine de la ressource ou des équipements mobiles concernés tant qu'une correction n'est pas identifiée et mise en place ? Comment déploie-t-on le correctif ?
- Afin de répondre aux obligations légales et réglementaires en vigueur, a-t-on défini une procédure de gestion et de notification des éventuelles violations de données en cas de faille de sécurité ?
- Quelles sont les conditions d'accès aux données de géolocalisation ?

14.3. Recommandations relatives à la sécurité

Les différents risques décrits dans le paragraphe précédent conduisent à émettre des recommandations en reprenant les groupes de service de l'architecture de référence définie au §5.2, dans le respect des dispositions du RGPD, de la loi informatique, fichier et libertés modifiée en 2018 et du Référentiel général de sécurité (RGS).

14.3.1. Gestion des équipements mobiles

RISQUE	RECOMMANDATION
Usage illicite du réseau Wi-Fi	▪ La fonction WPS (Wi-Fi Protected Setup) des points d'accès **DOIT** être systématiquement désactivée. ▪ Le code du réseau Wi-Fi **NE DOIT PAS** être divulgué.
Utilisation d'un système d'exploitation (ROM) alternatif (via USB par exemple)	▪ L'installation par l'utilisateur d'un système d'exploitation (ROM) alternatif **DEVRAIT** être interdite. ▪ Les systèmes d'exploitation (ROM) en cours de déploiement **DOIVENT** être surveillés depuis la fonction MDM. ▪ Un contrôle aléatoire des équipements mobiles **DEVRAIT** être mis en place.
Dépassement des limites de l'équipement mobile (mémoire vive ou capacités du processeur)	▪ L'éditeur **DOIT** spécifier les prérequis matériels (et autres incompatibilités) de ses ressources. ▪ L'académie et les collectivités **DOIVENT** définir ensemble le panier minimum d'applications (en impliquant les enseignants). ▪ Le matériel **DOIT** être choisi en fonction des ressources prévues. ▪ Les ressources choisies **DOIVENT** être supportées par le matériel. ▪ Les masters **DOIVENT** être compatibles avec le matériel (puissance requise et place totale occupée sur l'équipement mobile).
Données perdues	▪ L'image de l'équipement mobile (applications + données + configuration) à l'exception des équipements BYOD non gérés par un outil de gestion de parc (MxM) **DOIT** être sauvegardée, de manière sécurisée et dans le respect des dispositions légales et réglementaires en vigueur, pour restaurer un équipement mobile à l'identique. ▪ Les données de l'espace pédagogique **DOIVENT** être sauvegardées[26] de manière sécurisée et dans le respect des dispositions légales et réglementaires en vigueur. ▪ Les données de l'espace privé **NE DOIVENT PAS** être sauvegardées (la charte fera mention de cette exclusion).
Équipement mobile indisponible (volé ou perdu)	▪ L'équipement mobile **DEVRAIT** pouvoir être géolocalisé, dans le respect des dispositions légales et réglementaires, suite à une déclaration officielle de perte ou de vol effectuée par les responsables légaux et dans le cas d'une réquisition judiciaire. ▪ Des notifications **PEUVENT** être envoyées sur les équipements mobiles perdus ou volés. ▪ L'équipement mobile **DOIT** pouvoir être bloqué à distance. ▪ Les données de configuration (compte, Wi-Fi…) **PEUVENT** être supprimées à distance.

[26] À consulter CARINE version 1.0 (http://eduscol.education.fr/carine), chapitre 3.4.1, page 59.

Installation sur l'équipement mobile de logiciels malveillants (virus, vers, chevaux de Troie, logiciels espions)	▪ Le système d'exploitation de l'équipement mobile **DOIT** être maintenu en permanence à jour des correctifs de sécurité après validation du bon fonctionnement des applications sur la mise à jour (hors des heures de cours, pour éviter de bloquer les appareils). ▪ Des solutions d'analyse statistique de l'utilisation des ressources, du trafic réseau, **PEUVENT** être mises en place dans le respect des obligations légales et réglementaires. ▪ Un antivirus **DEVRAIT** être installé sur l'équipement mobile dès la phase de préparation.
Accès à la localisation de l'utilisateur	▪ La fonction géolocalisation de l'équipement mobile **DOIT** apparaître visiblement lorsqu'elle est activée et son activation **DOIT** recueillir le consentement de l'utilisateur.
Accès aux contacts	▪ Tout accès par une application à la liste de contacts de l'utilisateur **DOIT** recueillir le consentement de ce dernier.
Notifications	▪ Les applications proposant des notifications **DOIVENT** recueillir le consentement de l'utilisateur. ▪ Pour les applications préinstallées, les notifications **DOIVENT** être désactivées par défaut. ▪ Les paramétrages de notification des applications **DOIVENT** rester disponibles pour les utilisateurs.
Contrôle parental	▪ L'EIM **DEVRAIT** être équipé d'un outil de contrôle parental avec un paramétrage par défaut. Le code d'accès au paramétrage est fourni aux parents.

Tableau 5 : Sécurité - Risques et recommandations - Gestion des équipements mobiles

14.3.2. Services de gestion des productions numériques

RISQUE	RECOMMANDATION
Mélange des productions scolaires et privées	▪ L'EIM **DOIT** comporter un espace pédagogique. ▪ L'EIM **DOIT** comporter un espace privé pour les données privées. ▪ L'espace personnel **DOIT** être défini (exemple : emplacement, limites) et nommé sans ambiguïté (exemple : PERSONNEL). Des processus d'effacement irréversible des données **DOIVENT** être prévus pour chaque cas d'usage (changement d'utilisateur, fin de la durée de conservation prévue des données…). Les fichiers structurés de données à caractère personnel **DOIVENT** être stockés dans des espaces qui respectent la réglementation.[27]

[27] À consulter CARINE version 1.0 (http://eduscol.education.fr/carine), chapitre 3.4.1, page 59.

Accès et divulgation des productions personnelles	▪ L'accès à l'espace personnel d'un utilisateur **DOIT** lui être réservé, à l'exclusion de toute autre personne. Sans possession des moyens d'authentification de l'utilisateur, les données **NE DOIVENT PAS** pouvoir être consultées / modifiées. En particulier, les administrateurs techniques des espaces de stockage gèrent la capacité des espaces mais **NE DOIVENT PAS** accéder au contenu de l'espace personnel (clairement identifié comme tel) sans l'accord de l'utilisateur ou d'une autorité judiciaire.
Dépassement des limites de l'EIM (stockage interne ou carte mémoire additionnelle)	▪ Un seuil d'alerte **DEVRAIT** être défini pour prévenir l'utilisateur. Un seuil par espace (pédagogique et privé) **PEUT** être défini.
EIM perdu ou volé	▪ Les productions **DEVRAIENT** pouvoir être supprimées à distance. ▪ La solution MxM **DOIT** offrir la possibilité à l'utilisateur de supprimer ses données personnelles. ▪ La réinstallation du système d'exploitation par un utilisateur **DEVRAIT** être empêchée.

Tableau 6 : Sécurité - Risques et recommandations - Gestion des productions numériques

14.3.3. Distributions des applications mobiles

RISQUE	RECOMMANDATION
Installation non autorisée d'applications mobiles	▪ L'accès aux systèmes d'installation des applications par profil (enseignant versus élève) **DOIT** être contrôlé. ▪ L'administrateur local de l'établissement ou de l'école **DOIT** pouvoir mettre à jour le store privé avec les applications achetées par l'établissement ou l'école. ▪ Les élèves et les enseignants **DOIVENT** pouvoir installer, désinstaller ou mettre à jour une application depuis un magasin privé. ▪ La fonction MAM **DEVRAIT** permettre d'interdire l'accès à certaines applications (par exemple : store). ▪ La solution MxM **DEVRAIT** pouvoir contrôler l'accès au paramétrage de l'équipement mobile.
Impossibilité de distribuer les applications (service indisponible, temps de déploiement trop long)	▪ La solution de distribution des applications mobiles **DOIT** proposer un service fiable et réactif.

Tableau 7 : Sécurité - Risques et recommandations - Distribution des applications mobiles

14.3.4. Services d'infrastructure pour l'établissement

Il s'agit des services suivants :

- service d'authentification ;
- service d'annuaire ;
- service de stockage ;

- service de supervision et d'exploitation de l'infrastructure ;
- service de gestion des journaux.

⇨ Ces services sont à définir en partenariat entre les collectivités et l'académie sur la base des préconisations des référentiels type CARINE et référentiel Wi-Fi (cf. chapitres 4.2 « S2I2E – CARINE » et 4.1 « Référentiel Wi-Fi »)

Ces prérequis **DOIVENT** être mis en place dans le respect des dispositions légales et réglementaires.

Une attention particulière est à porter sur le nombre d'adresses IP nécessaires pour intégrer l'ensemble des équipements mobiles sur le réseau de l'établissement.

14.3.5. Services de sécurité

RISQUE	RECOMMANDATION
Accès à des données personnelles/confidentielles	▪ L'accès à l'équipement mobile **DOIT** être sécurisé, par exemple par un mot de passe répondant aux recommandations notamment de l'ANSSI et de la Cnil. ▪ Un verrouillage du terminal avec une mise en veille sécurisée au bout d'une inactivité de quelques minutes **DOIT** être proposé. ▪ L'EIM (hors terminaux BYOD) **DEVRAIT** être protégé par l'identifiant de connexion et le mot de passe du compte ENT. ▪ Au-delà du contrôle d'accès à l'équipement mobile, l'accès aux applications comportant des données personnelles **DEVRAIT** être sécurisé. ▪ Les applications pouvant être téléchargées sur l'équipement mobile **DEVRONT** respecter le principe de demande d'autorisation préalable de l'utilisateur avant d'accéder à ses fichiers.
Utilisation non conforme de l'équipement mobile par l'utilisateur	▪ Le dispositif conventionnel **DOIT** préciser aux utilisateurs les conditions d'utilisation de l'équipement mobile.

Tableau 8 : Sécurité - Risques et recommandations - Services de sécurité

14.4. Authentification

L'authentification s'opère principalement sur 3 niveaux distincts :

- sur l'équipement mobile, pour déverrouiller l'accès au terminal ;
- sur les ressources :
  - les applications mobiles : pour lesquelles une authentification par login/mot de passe ou par code d'activation est possible,
  - les ressources de type fichier stockées sur des serveurs distants ;
- sur le réseau, principalement l'accès au réseau Wi-Fi de l'établissement ou de l'école :
  - se référer au référentiel CARINE et au référentiel Wi-Fi pour les modalités de mise en œuvre (cf. chapitres 4.2 « S2I2E – CARINE » et 4.1 « Référentiel Wi-Fi »).

Concernant les applications mobiles, il est possible de mettre en place des mécanismes de *SSO* (Single Sign-On) qui permettent de s'authentifier une fois et d'utiliser une ou plusieurs autres applications sans avoir à s'authentifier à nouveau.

Les éditeurs d'application **PEUVENT** proposer des applications respectant ce mécanisme de *SSO*. Cela garantit un plus grand confort d'utilisation.

Pour les traitements de données biométriques qui répondent aux conditions déterminées notamment par la Cnil, le responsable de traitement **DOIT**, avant tout déploiement, réaliser une analyse d'impact (AIPD) et recueillir d'une manière adaptée le consentement de la personne concernée. Ceci concerne, par exemple, la reconnaissance d'empreinte digitale ou faciale.

En cas d'utilisation de moyens d'identification et authentification basés sur des données biométriques (images d'empreintes, images d'iris…), les terminaux **NE DOIVENT PAS** stocker en clair ces données et **NE DOIVENT PAS** les envoyer vers un système d'authentification extérieur sous cette forme. Ils **NE DEVRAIENT PAS** les envoyer, même chiffrées ou hachées, vers un système extérieur et les y stocker, sauf justification impérative à inscrire explicitement au registre des traitements. Des recommandations CNIL et ANSSI existent à ce propos[28][29].

14.5. Autorisations

La notion d'autorisation est présente à plusieurs niveaux :

- sur le contenu : l'accès au contenu répond à des règles d'autorisation en accès, lecture ou écriture. Ceci est valable pour un contenu local à l'équipement mobile ou distant ;
- sur les ressources présentées : seules les ressources auxquelles l'utilisateur a droit lui sont présentées ;
- sur l'équipement mobile : selon le *profil* utilisateur les autorisations sur l'utilisation de l'équipement mobile seront différentes (autorisation d'installer ou désinstaller une application mobile, autorisation de changer la configuration de l'équipement mobile…).

14.6. Alimentation des MxM et des outils de gestion de classe en données

14.6.1. Modes d'alimentation des solutions MxM et gestion de classe

Les solutions de MxM et de gestion de classe ont besoin pour leur propre fonctionnement d'informations concernant les utilisateurs et les groupes d'utilisateurs auxquels ils appartiennent (cf. § 7.2.2 « Gestion des profils utilisateur ».

Plusieurs modalités d'alimentation peuvent être mises en œuvre : saisie directe (mode autonome), import des données, accès direct à un référentiel d'identité.

Le choix du mode d'interfaçage entre les solutions de MxM et le référentiel d'identité dépend de différentes contraintes :

- des contraintes techniques de faisabilité propres aux solutions de MxM / gestion de classe retenues ;
- des contraintes sur le besoin de fraîcheur des données ou sur les performances d'accès.

[28] https://www.cnil.fr/fr/declaration/au-053-biometrie-controle-dacces-sur-les-lieux-de-travail-avec-conservation-des-gabarits

[29] https://www.cnil.fr/fr/declaration/au-052-biometrie-controle-dacces-sur-les-lieux-de-travail-avec-maitrise-de-la-personne

Dans tous les cas :

- seules les informations nécessaires au fonctionnement de la solution de MxM ou de gestion de classe **DOIVENT** être exploitées. Les principes légaux de proportionnalité, de finalité et de minimisation **DOIVENT** être respectés ;
- le référentiel d'identité sera de préférence le référentiel le plus complet et le plus à jour de ces données (par exemple celui de l'*ENT* qui intègre l'ensemble des groupes mis en œuvre dans l'établissement). Les recommandations relatives aux référentiels d'identité qui peuvent être interrogés sont décrites au paragraphe 14.6.3.

14.6.1.1. Saisie directe (mode autonome)

Les solutions de MxM et de gestion de classe permettent de créer les identités et les groupes de manière unitaire, par saisie directe dans l'outil.

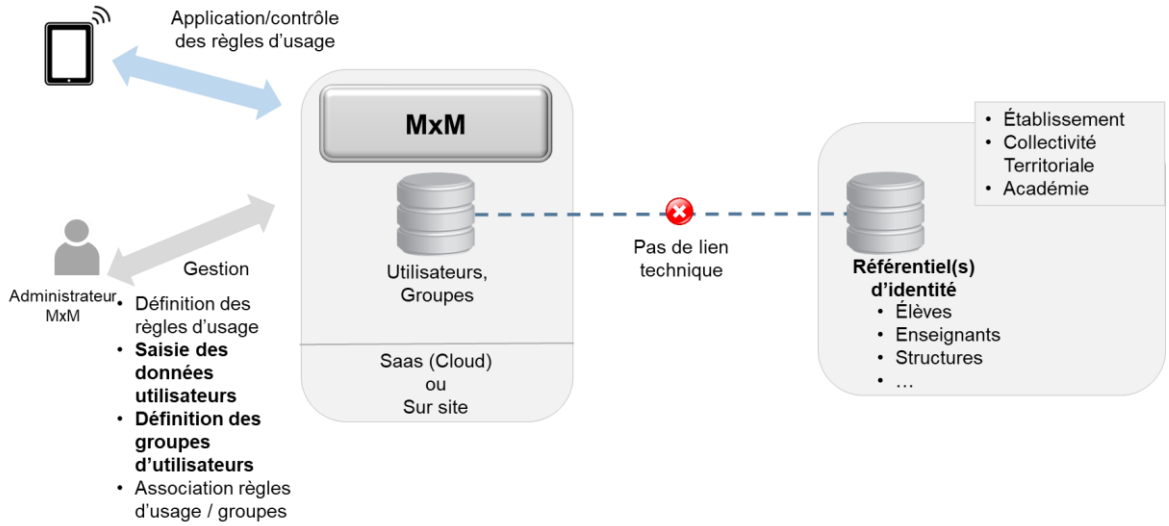


Illustration 21 : Cas d'un MxM autonome

14.6.1.2. Import des données

Il est cependant recommandé d'interfacer la solution MxM ou de gestion de classe avec un référentiel déjà mis en place afin d'y intégrer les données uniquement pertinentes et nécessaires relatives aux utilisateurs de la communauté éducative de chaque établissement.

Pour ce faire, les solutions de MxM ou de gestion de classe proposent des fonctions d'import.

Les deux modes (autonome, import) peuvent être combinés, selon le contenu du (ou des) référentiel(s) d'identité utilisés et la compatibilité des formats (par exemple, import des données utilisateurs depuis un annuaire externe et saisie des groupes directement dans la solution MxM/gestion de classe).

Les données présentes dans la solution de MxM ou gestion de classe doivent être actualisées en intégrant les mouvements (d'élèves, d'enseignants, de groupes…), soit de façon manuelle (par saisie), soit par rafraichissement automatisé périodique (imports périodiques).

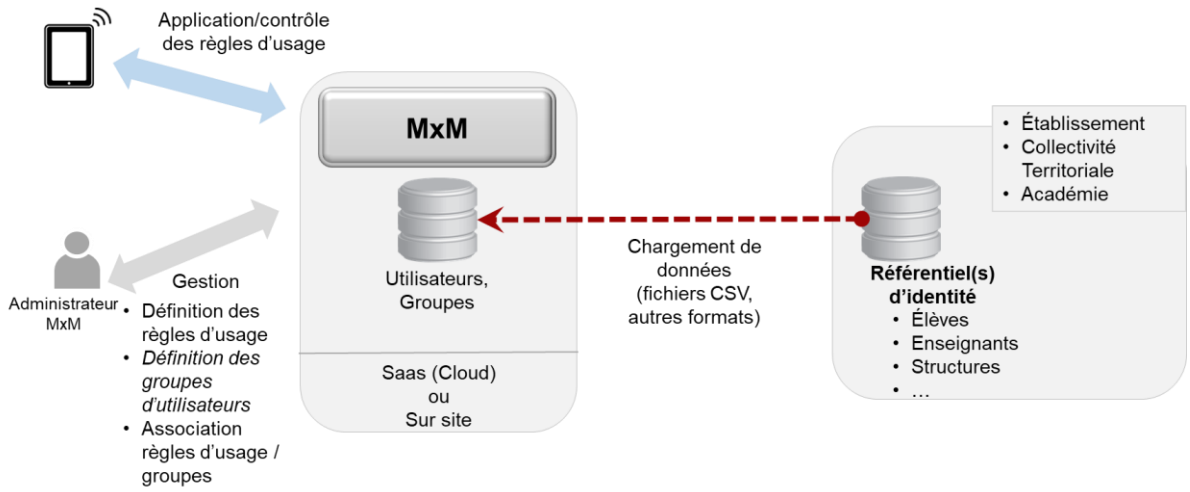


Illustration 22 : Cas d'import de données utilisateurs dans un MxM depuis un référentiel d'identité

14.6.1.3. Accès direct à un référentiel d'identité

Dans un mode intégré, la solution de MxM / gestion de classe se connecte à un référentiel d'identité qu'elle interroge pour obtenir les données nécessaires, afin de couvrir les différents cas d'usages identifiés dans le contexte du projet, c'est-à-dire permettre de regrouper des populations dans des ensembles auxquels appliquer des règles de gestion communes.

Les recommandations relatives aux référentiels d'identité qui peuvent être interrogés sont décrites au paragraphe 14.6.3.

Les solutions de MxM / gestion de classe **DOIVENT** offrir des mécanismes sécurisés (protocoles et formats d'échange) d'intégration avec des annuaires externes ; on retrouve souvent LDAP ou Active Directory.

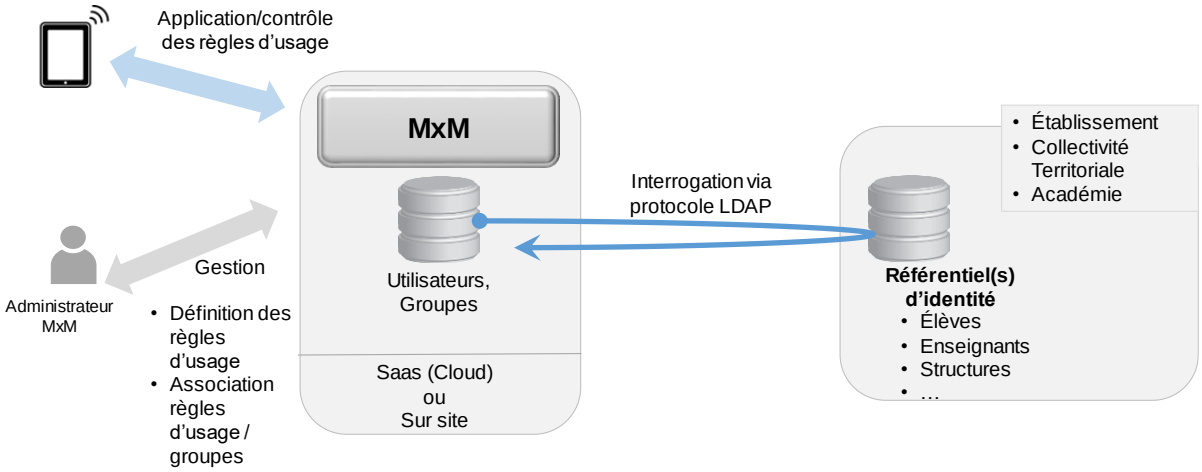


Illustration 23 : Cas de l'accès direct d'un MxM à un référentiel d'identité

14.6.2. Caractéristiques des données

Le tableau ci-après inventorie tout ou partie des données à caractère personnel susceptibles d'être traitées par les solutions de MxM / gestion de classe pour leurs besoins propres. Les données traitées doivent être strictement nécessaires au fonctionnement des solutions et pour les usages définis. Elles ne doivent, en aucun cas, être utilisées pour d'autres finalités que celles prévues.

Il comprend les colonnes suivantes :

- Attribut : nom courant de l'attribut (indiqué en gras si obligatoire, en italique si multivalué) ;
- Type : catégorie d'attribut ;
- Libellé : Nom de l'attribut - Fourni à titre indicatif seulement (chaque solution dispose de sa propre codification) ;
- Justification / commentaires : indique l'usage potentiel qui justifie le besoin de disposer de cet attribut et/ou apporte une précision ;
- Obl / Fac : indique si l'attribut doit obligatoirement être renseigné (Obl pour obligatoire) ou s'il peut être laissé vide (Fac pour facultatif). Il est précisé que les données qualifiées facultatives ne peuvent être traitées que dans le respect des principes légaux de minimisation et de proportionnalité ;
- Mo / Mu : indique si l'attribut est monovalué (Mo) ou multivalué (Mu).

Libellé	Type	Code	Justification / commentaires	Obl / Fac	Mo / Mu
Identifiant du matériel	technique	EimIdentifiant	Après association de l'EIM à la personne physique, permet indirectement l'identification de la personne physique	Obl	Mo
Attributs uniques à un matériel	technique	Libre	Les attributs propres au matériel ou à un de ses composants (adresse MAC, numéro de série, IMEI…) permettent indirectement l'identification de la personne physique	-	-
Identifiant de l'utilisateur	technique	PersonIdentifiant	Identifier l'utilisateur "propriétaire" de l'EIM. Pour les élèves, cet identifiant ne peut être une adresse e-mail	Obl	Mo
Profils de l'utilisateur	technique	PersonProfils	Profils auxquels appartient la personne. Permet d'affecter la personne à un groupe MDM et déterminer les droits associés	Fac	Mu
Nom d'usage	civilité	PersonNom	Sert à identifier la personne pour l'affecter dans les groupes MDM. Utile aussi aux fonctions de gestion de classe	Fac	Mo
Prénom usuel	civilité	PersonPrenom	Sert à identifier la personne pour l'affecter dans les groupes MDM. Utile aussi aux fonctions de gestion de classe	Fac	Mo
Adresse mail	coordonnées	PersonMail	Selon le contexte d'usage. Nota : pas d'adresse mail pour les élèves	Fac	Mo
Structure de rattachement	coordonnées	PersonStructRattach	Établissement ou école de rattachement de l'élève. Des règles de gestion peuvent être différentes selon les établissements.	Fac	Mo
Établissements d'exercice	coordonnées	EnsStructExercice	Établissements dans lesquels exerce l'enseignant	Fac	Mu
Niveau	scolarité	EleveNiveau	Pour les élèves. Exemples : 5e, 4e… Les règles de gestion ou de distribution peuvent être différentes selon les niveaux	Fac	Mo
Discipline enseignée	scolarité	EnsDiscipline	Pour les enseignants. Exemple : français, mathématiques, EPS…	Fac	Mu
Classe (division)	coordonnées	EleveClasse	Classe (division) dans laquelle est inscrit l'élève. Pour les fonctions de gestion de classe.	Fac	Mo
Groupes d'appartenance	coordonnées	EleveGroupes	Groupes dans lesquels est inscrit l'élève. Pour les fonctions de gestion de classe.	Fac	Mu
Mot de passe de l'EIM	technique	EimMotDePasse	Pour certaines fonctions de sécurité et uniquement sous la forme cryptée.	Fac	Mo

Tableau 9 : Dictionnaire de données à caractère personnel utilisables dans les outils de MxM / gestion de classe

14.6.3. Référentiels d'identité utilisables

Les solutions de gestion de parc (MxM et/ou gestion de parc informatique) et les services de gestion de classe **PEUVENT** être alimentés à partir de référentiels d'identité préexistants, mais **NE DOIVENT** reprendre que les données strictement nécessaires à leurs fonctions.

Les sources de données envisageables sont les suivantes :

- l'Annuaire Académique Fédérateur (AAF), sous réserve qu'il fasse l'objet d'une extraction spécifique[30] ;
- l'annuaire ENT, sous réserve qu'il soit fourni dans le cadre d'un partenariat État – collectivité territoriale et que l'engagement de conformité au RU-003 ait été réalisé par le responsable de traitement.

Dans tous les cas, pour mettre en œuvre l'alimentation à partir de ces sources et à partir d'autres référentiels, les responsables de traitement **DOIVENT** s'assurer que :

- conformément au RGPD, les destinataires et émetteurs du flux sont bien identifiés (fiches de traitement inscrites dans le registre des traitements du responsable de traitement) ;
- les personnes concernées ont été informées conformément aux dispositions légales et réglementaires de cette communication.

L'alimentation doit s'effectuer de manière sécurisée par des mesures techniques et organisationnelles appropriées pour assurer la sécurité et la confidentialité des données.

[30] Il est recommandé d'utiliser l'export AAF spécifique nommé GPEI (Gestion des Parcs des Équipements Informatiques) qui est le résultat d'un traitement national. Les solutions de gestion de parc et les services de gestion de classe qui envisagent de s'alimenter à partir de cet export doivent être conformes aux cadres de référence CARMO et CARINE.

15. Services d'infrastructure pour l'établissement

15.1. Liste des services attendus (fonctionnalités)

Les services accessibles via un équipement mobile sont organisés en 3 catégories.

- Les services d'infrastructure :
  - service d'annuaire ;
  - service poste de travail ;
  - service d'authentification ;
  - service de sécurité et d'accès réseau ;
  - service de diffusion d'information.
- Les services de maintien en condition opérationnelle :
  - service de sauvegarde ;
  - service de régénération et de configuration de stations ;
  - service de supervision et d'exploitation de l'infrastructure ;
  - service de gestion des journaux ;
  - service de gestion de parc.
- Les services rendus aux utilisateurs :
  - service de stockage ;
  - service de messagerie électronique ;
  - service de communication temps réel ;
  - service de publication ;
  - service de recherche documentaire.

Ces services sont détaillés dans le cadre de référence S2I2E - CARINE (cf. paragraphe 4.2 « S2I2E – CARINE »).

15.2. Impact organisationnel (rôles et acteurs)

La mise en place des équipements mobiles et des services associés s'inscrit dans la continuité des recommandations S2I2E - CARINE.

15.3. Modalités opérationnelles

Les modalités opérationnelles sont détaillées dans le cadre de référence S2I2E - CARINE (cf. paragraphe 4.2 « S2I2E – CARINE »).

16. Gestion des productions numériques (communément appelée *MCM*)

Cette partie concerne les porteurs de projet qui doivent commander l'outil portant les fonctions de gestion des productions numériques associé au choix de l'équipement mobile (*MCM*).

Les productions numériques peuvent être stockées en plusieurs endroits différents selon les situations et l'existant informatique de l'école ou l'établissement, principalement :

- sur l'équipement mobile, indifféremment sur la mémoire interne ou une carte mémoire additionnelle ;
- sur des serveurs mis à disposition par les porteurs de projet ;
- via des services de stockage tiers. Nous appellerons ce type de stockage un stockage en nuage pour reprendre un terme largement répandu.

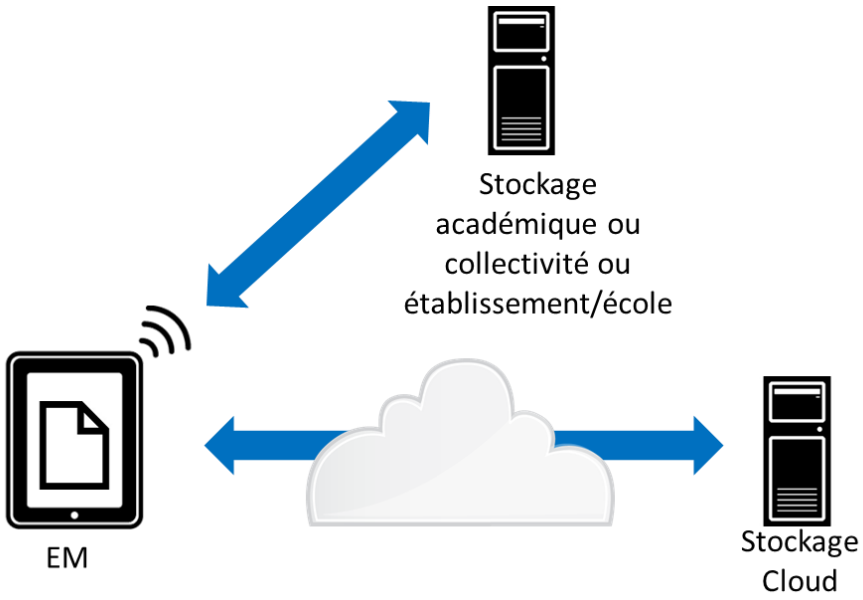


Illustration 24 : Stockage des productions numériques

16.1. Liste des services attendus (fonctionnalités)

Quel que soit le type de stockage choisi pour les productions numériques, il y a nécessité de disposer d'un espace sécurisé de stockage des productions élèves et enseignants. La solution mise en œuvre **DOIT** prévoir un espace de stockage des productions numériques.

La fonction de MCM **DOIT** permettre aux utilisateurs d'ajouter, de modifier et de supprimer des travaux qu'ils ont réalisés.

Dans les cas où l'établissement ou l'école a décidé de permettre à l'élève d'utiliser l'équipement mobile dans un cadre privé (valable également dans le cas du BYOD), l'EIM **DOIT** comporter un espace individuel, privé, pour les données privées (cette recommandation est valable également dans les projets BYOD s'appuyant sur une solution de MxM). Et dans tous les cas où l'équipement mobile est pris en charge par une solution MxM, l'EIM **DOIT** comporter un espace spécifique dit « espace pédagogique » associé aux activités scolaires.

Si un espace privé existe, il **DOIT** être défini : en précisant son emplacement et ses limites. Les données privées de l'utilisateur **DOIVENT** être identifiées par les mots "PERSONNEL" ou "PRIVÉ" (nom de répertoire ou de fichier, en-tête de message…).[31]

Le stockage de données est soumis à des limites, quel que soit l'emplacement du stockage (équipement mobile, serveur distant infogéré ou non). Pour éviter le dépassement de ces limites et des problèmes de réalisation des usages pédagogiques, des seuils d'alerte **DOIVENT** être définis pour informer l'utilisateur qu'il s'approche de la limite de son volume de stockage attribué et disponible.

Si l'espace de stockage est externalisé, un système de quotas **DOIT** être mis en œuvre par profil (élève/enseignant) pour éviter un dépassement des limites des serveurs de stockage et une éventuelle surfacturation des services.

Pour garantir la continuité des usages indépendamment du type de terminal utilisé, les productions **DEVRAIENT** être accessibles depuis différents terminaux (équipement mobile, PC via *ENT* par exemple).

La solution retenue pour la fonction MCM **DEVRAIT** pouvoir s'interfacer avec le référentiel d'identité afin de ne pas multiplier les comptes pour les utilisateurs.

Quel que soit le type de stockage privilégié :

- l'accès aux productions **DOIT** être contrôlé en lecture et en écriture pour respecter les droits d'accès ; l'authentification doit donc être vérifiée (login/mot de passe, authentification par l'équipement mobile…) et l'autorisation contrôlée ;
- les services de stockage **DOIVENT** utiliser un antivirus régulièrement mis à jour pour garantir la sécurité.

16.2. Impact organisationnel (rôles et acteurs)

L'organisation va principalement concerner la gestion du prestataire responsable du stockage et des outils associés.

Une personne aura la charge de veiller :

- au respect des règles de sécurité ;
- à ce que le contrat choisi soit conforme aux exigences du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018 et contenir les dispositions adéquates pour assurer la sécurité et la confidentialité des données à caractère personnel ;
- à ce que le contrat choisi soit cohérent avec les usages.

Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** inscrire l'ensemble des traitements dans son registre des traitements dans le respect des dispositions légales et réglementaires. Voir au § 21.2.6.

16.3. Modalités opérationnelles

Certaines recommandations sont particulières dans les cas où le stockage est infogéré :

- une plage de service et de maintenance **DOIT** être définie ;
- la disponibilité d'accès attendue durant la plage de service **DOIT** être définie avec un taux proche de 99% ;

[31] À consulter CARINE version 1.0 (http://eduscol.education.fr/carine), chapitre 3.4.1, page 59.

- l'infogérance **DOIT** anticiper la montée en charge en rapport avec les phases de déploiement des équipements mobiles dans l'établissement ou l'école si le déploiement est progressif ;
- les données **DOIVENT** être sauvegardées ;
- des capacités de restauration de données **DOIVENT** être proposées dans le service ;
- un contrat d'hébergement en bonne et due forme **DOIT** être proposé pour encadrer la prestation.

Dans le cas où les productions numériques sont accessibles depuis différents terminaux (équipement mobile, PC…) le format des productions **DOIT** être utilisable quel que soit le terminal (en lecture ou en lecture/écriture).

Un utilisateur **DOIT** pouvoir disposer d'un temps raisonnable (par exemple 3 mois) pour récupérer ses productions numériques dans le cas d'un départ en cours d'année scolaire.

D'une manière générale, les droits des personnes concernées par le traitement des données à caractère personnel tels que prévus dans le RGPD et la loi informatique, fichier et libertés modifiée en 2018 doivent être assurés dans tout projet de déploiement d'équipements mobiles, en particulier en matière de gestion des productions numériques. Des procédures permettant l'exercice des droits des personnes doivent être déployées par les responsables de traitement, étant précisé que les responsables de traitement disposent d'un délai d'un mois à compter de la réception de la demande d'exercice d'un droit pour y répondre sauf exception.

17. Services fonctionnels de gestion de classe

Les services de gestion de classe permettent à l'enseignant d'organiser, d'administrer, de surveiller les séquences pédagogiques dans lesquelles ses élèves utilisent des équipements mobiles.

Ces services sont proposés dans des outils spécialisés ; on les trouve également dans certaines solutions de MxM, dont les autres fonctions sont évoquées aux chapitres 12, 13, 16.

17.1. Liste des services attendus (fonctionnalités)

L'enseignant **DOIT** pouvoir diffuser une ressource aux élèves de sa classe.

L'enseignant **DOIT** pouvoir autoriser, restreindre ou bloquer temporairement les accès à internet des élèves, en fonction des objectifs pédagogiques de la séquence.

L'enseignant **DEVRAIT** pouvoir visualiser sur son poste de travail ou équipement mobile l'écran de ses élèves. Ceci afin de s'assurer de l'avancement des travaux, d'identifier les élèves ayant besoin d'aide.

L'enseignant **DEVRAIT** pouvoir diffuser l'écran de son poste de travail ou équipement mobile sur l'écran des équipements mobiles de ses élèves. Ceci afin de s'assurer d'une diffusion ciblée, de qualité et à un rythme contrôlé des éléments affichés sur son poste de travail ou d'une diffusion collective en l'absence de moyens dédiés.

L'enseignant **DEVRAIT** pouvoir bloquer à distance les équipements mobiles des élèves, afin d'éviter les distractions lorsque l'équipement mobile n'est pas utilisé en cours.

L'enseignant **DOIT** pouvoir autoriser ou bloquer certaines applications, pour un travail particulier, ou lors d'un contrôle.

L'enseignant **DEVRAIT** pouvoir consulter la liste des équipements mobiles de sa classe ainsi que leur état (batterie, connectivité) afin de s'assurer de leur disponibilité pour tous les élèves.

L'enseignant **PEUT** créer des enquêtes anonymes ou pseudonymisées et consulter le résultat.

L'enseignant **DEVRAIT** pouvoir créer des groupes virtuels.

L'enseignant **PEUT** bloquer ou autoriser la copie de données depuis ou vers un périphérique de type carte *SD* ou clé USB.

L'enseignant **PEUT** autoriser un élève à afficher ce qu'il fait sur l'écran des autres équipements mobiles de la classe ou d'un groupe.

L'enseignant **PEUT** diffuser simultanément une sélection de fichiers de formats divers (audio, vidéo, image, texte, PDF…) à tous les élèves ou un groupe.

L'enseignant **DEVRAIT** pouvoir en un clic assombrir l'écran des équipements mobiles pour capter l'attention ou réduire la luminosité dans la classe lors d'une projection avec un vidéoprojecteur.

L'enseignant **PEUT** mettre en place des sessions de discussion.

L'enseignant **DEVRAIT** pouvoir utiliser son micro pour parler à un élève ou un groupe.

L'enseignant **DEVRAIT** pouvoir écouter ce que dit un élève dans son micro.

L'enseignant **DEVRAIT** pouvoir, de façon simple, apporter des commentaires écrits enregistrables sur l'interface élève de l'équipement mobile.

L'enseignant **DOIT** pouvoir collecter facilement un travail fait par les élèves (audio, vidéo ou document).

Les fonctionnalités de gestion de classe **NE DOIVENT PAS** être utilisées à des fins de mesure d'activité ou de capacités cognitives de l'élève en dehors d'un cadre expérimental et contractuel où les sous-traitants de la solution s'engagent sur l'hébergement et l'exploitation des données à des fins éducatives pédagogiques (valorisation des données).

L'ENT et l'EIM **DEVRAIENT** partager un espace de stockage qui **DOIT** être associé au profil de l'utilisateur dès son authentification.

17.2. Impact organisationnel (rôles et acteurs)

Si certains de ces services peuvent être utilisés lors de la préparation de cours, éventuellement avec l'aide d'un tiers, ils sont généralement mis en œuvre par l'enseignant devant ses élèves.

Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** inscrire l'ensemble des traitements dans son registre des traitements dans le respect des dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018. Voir au §21.2.6.

17.3. Modalités opérationnelles

Les fonctionnalités de la solution de gestion de classe **DOIVENT** être simples d'emploi et efficaces. Utilisés pendant les cours, elles ne doivent pas générer de perte de temps ou d'interruptions pour des manipulations compliquées ou des délais d'activation.

La solution de gestion de classe **DEVRAIT** également intégrer les autres matériels connectés (p.ex. : vidéoprojecteur, TBI).

Les enseignants **DOIVENT** avoir été formés (cours ou auto apprentissage) à la manipulation des équipements mobile.

Dans le respect notamment des principes de finalité, de proportionnalité et de minimisation des données définis par le RGPD et la loi informatique, fichiers et libertés modifiée en 2018, la solution de gestion de classe **DOIT** être capable de s'intégrer au référentiel d'identité ou au référentiel utilisé par la solution de MxM.

18. Support logiciel

18.1. Liste des services attendus (fonctionnalités)

Un guichet d'assistance logicielle **DOIT** être mis à disposition des utilisateurs.

Ce guichet **DOIT** a minima proposer une assistance téléphonique pour répondre aux sollicitations des enseignants, du personnel académique ou de la collectivité territoriale, ou encore des élèves et de leurs parents.

Pour éviter d'avoir recours systématiquement à une assistance téléphonique et pour gagner du temps, le guichet d'assistance **DOIT** également proposer un portail en ligne comprenant des tutoriels, une rubrique « questions fréquentes », un forum ou encore une messagerie instantanée.

Ce portail d'assistance **DEVRAIT** être positionné sur l'écran d'accueil de l'équipement mobile comme raccourci lors de la préparation de l'équipement mobile. Ainsi l'utilisateur aura un accès direct à l'assistance.

Le formulaire de demande d'assistance, de forum ainsi que la rubrique « questions fréquentes » **DOIVENT** être accessibles en dehors des heures ouvrables.

18.2. Impact organisationnel (rôles et acteurs)

L'organisation du support peut être organisée selon plusieurs niveaux d'expertise.

Par exemple, on peut imaginer une organisation à 3 niveaux :

- un premier niveau en établissement ou en école pour répondre aux problèmes récurrents et connus ; ce contact n'est pas téléphonique mais physique, l'élève ou l'enseignant va directement consulter la personne en charge du support ;
- un deuxième niveau pris en charge par la collectivité territoriale ou l'académie ou le prestataire ; ce deuxième niveau est consultable par téléphone et possède un niveau d'expertise plus poussé qu'en établissement ou en école ; dans le cas où le problème n'est pas résolu l'utilisateur est invité à contacter le niveau suivant, le niveau éditeur ;
- un troisième et dernier niveau pris en charge par l'éditeur de la ressource ; l'éditeur est le plus à même de répondre aux situations non résolues par les deux premiers niveaux - il a l'expertise la plus poussée et des outils comme les logs de ses serveurs.

Dans tous les cas, un document de type « convention de mise à disposition et d'utilisation » **DEVRAIT** décrire les modalités d'accès au support lorsque ce dernier peut être directement sollicité par un élève ou un parent (cf. §21.2.6).

18.3. Modalités opérationnelles

L'assistance téléphonique proposée par la collectivité, l'académie ou l'éditeur de la ressource **DOIT** être ouverte durant des horaires en cohérence avec les besoins des utilisateurs, donc a minima pendant les heures de classe et s'exécuter dans un cadre contractuel conforme au RGPD et la loi informatique, fichiers et libertés modifiée en 2018 en assurant notamment la sécurité et la confidentialité des données.

19. Classes mobiles

19.1. Liste des services attendus (fonctionnalités)

19.1.1. Conteneur

La configuration des salles et des bâtiments **DOIT** être prise en compte lors de la sélection du conteneur afin d'assurer les déplacements requis par l'usage prévu. Par exemple, un chariot lourd sera difficilement déplacé d'un étage à l'autre par les escaliers.

Le conteneur **DOIT** disposer d'un dispositif de rechargement électrique des équipements mobiles.

Si ce dispositif de rechargement électrique nécessite de relier les équipements mobiles au conteneur via des câbles, ceux-ci **DOIVENT** avoir une taille suffisante, afin d'assurer correctement leurs fonctions et non excessive pour ne pas risquer d'être sectionnés lors de la fermeture du conteneur.

Le conteneur **DOIT** pouvoir être relié au courant électrique et au réseau même lorsqu'il est fermé et sécurisé ; ceci afin de permettre les opérations de chargement électrique et de mise à jour des terminaux. Outre la connectique extérieure, une bonne ventilation du conteneur est nécessaire pour que les appareils puissent se recharger capot fermé.

Le conteneur **DOIT** posséder l'équipement adéquat pour ranger les câbles extérieurs lors des déplacements, afin de réduire les risques liés à l'encombrement ou aux accrochages.

Le volume de rangement du conteneur **DOIT** prendre en compte le volume des accessoires disponibles afin d'assurer le rangement de l'ensemble du matériel.

19.1.2. Équipements mobiles et accessoires

Pour l'usage en classe mobile, un accessoire **DEVRAIT** permettre de brancher deux casques en même temps sur un même équipement mobile.

L'acquisition complémentaire d'accessoires (chargeurs…) est à envisager pour permettre une utilisation des équipements mobiles sans le conteneur (par exemple : sortie scolaire sur plusieurs jours, dotation des équipements pour un usage individuel…).

19.1.3. Wi-Fi

Dans le cas où l'établissement n'est pas équipé d'un Wi-Fi sédentaire, la classe mobile **DOIT** être équipée d'une borne Wi-Fi pour relayer le réseau (accessible depuis une prise RJ45).

La borne Wi-Fi utilisée avec une classe mobile **DOIT** pouvoir être activée ou désactivée facilement par l'enseignant (par exemple via un interrupteur).

Dans le cas où l'établissement n'est pas équipé d'un Wi-Fi sédentaire, une seconde borne amovible **PEUT** être ajoutée au dispositif afin d'assurer un usage simultané sur plusieurs classes et apporter une solution au manque de prises RJ45.

19.1.4. Gestion des équipements mobiles

Le matériel et les applications disponibles dans le cadre d'une classe mobile **DEVRAIENT** être gérés via des solutions de MxM.

Le déploiement de mises à jour et d'applications **DEVRAIT** être programmé en dehors des plages d'utilisation des terminaux de la classe mobile.

L'automatisation complète de la distribution des mises à jour est à privilégier (afin d'éviter les interventions manuelles comme déverrouiller l'équipement mobile) ; l'identification de différents niveaux de mise à jour (criticité, urgence) permet de programmer les mises à jour à différents moments définis dans l'organisation du projet.

19.2. Impact organisationnel (rôles et acteurs)

L'enseignant **DEVRAIT** disposer d'un équipement dédié.

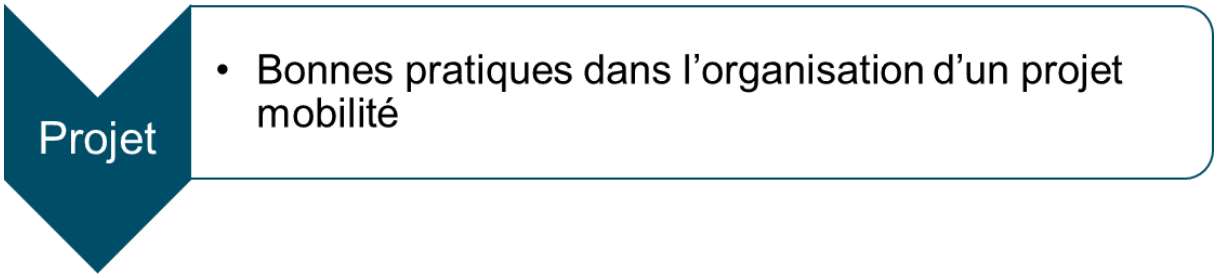
Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** inscrire l'ensemble des traitements dans son registre des traitements dans le respect des dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en. Voir au §21.2.6.

Dans le cas où une utilisation des terminaux dans le cadre périscolaire est envisagée, une convention co-rédigée par le directeur d'école et le responsable de l'équipe d'animation **DEVRAIT** être mise en place.

19.3. Modalités opérationnelles

Le lieu de stockage **DOIT** permettre le branchement électrique et l'accès au réseau (afin de permettre le rechargement des équipements mobiles et d'y appliquer des mises à jour en dehors des heures de classe).

Les utilisateurs d'une classe mobile **DOIVENT** disposer d'un espace sécurisé de stockage externe au terminal permettant de conserver les productions des élèves et de les retrouver à chaque séance.


Projet
• Bonnes pratiques dans l'organisation d'un projet mobilité

20. Observation des usages

Le succès d'un projet numérique ne se mesure pas au nombre d'équipements en service, mais aux usages qui en sont faits.

Pour évaluer les usages, plusieurs types d'informations sont nécessaires :

- des informations de contexte (*quel contexte aux usages ?*) ;
- des informations sur les utilisations (*quels services/outils numériques utilisés et par quel profil d'utilisateurs* ?) ;
- des informations permettant d'évaluer la contribution des outils numériques aux usages pédagogiques *(dans quels objectifs ? avec quelle efficacité ?*).

Les informations d'utilisation peuvent être collectées, analysées, en vue d'en tirer des axes d'amélioration au bénéfice de l'usager dans le respect des dispositions légales et réglementaires en matière de protection des données à caractère personnel.

.

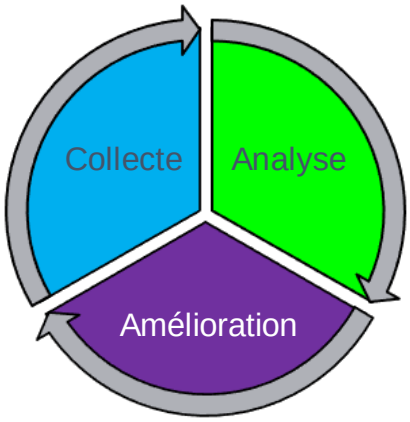


Illustration 25 : Cycle d'observation des usages

20.1. Remontée d'informations sur les utilisations

Il existe deux grandes formes de remontée d'informations sur les utilisations :

- la remontée automatique qui repose sur les rapports des différents outils impliqués dans l'écosystème :
  - l'outil de **gestion des équipements mobiles** (*MDM*) : cet outil donne des informations variées, telles que le nombre d'équipements mobiles ne respectant pas les politiques de sécurité ainsi que la nature de l'infraction, le taux d'occupation mémoire ou d'utilisation du processeur, l'espace disque occupé / disponible… Un tel outil peut être utilisé lorsqu'il y a recours à la gestion de parc d'équipements BYOD,
  - l'outil de **distribution des applications mobiles** (*MAM*) **:** cet outil est à même de donner des informations relatives aux applications utilisées par les élèves et les enseignants (nombre d'applications par équipement mobile, taille moyenne, versions utilisées),
  - l'outil de gestion des productions numériques (*MCM*) : espace consommé,

- les **ressources** : les applications mobiles peuvent remonter aux éditeurs de l'application certaines informations très utiles comme le nombre d'ouvertures de l'application sur des périodes, le ratio d'utilisation en mode connecté / non connecté, les échecs d'authentification, des dysfonctionnements parce que l'équipement mobile dépasse ses capacités (de traitement ou de stockage…) ;

- la collecte manuelle, dont les sources sont très variées :
  - les **élèves** et les **enseignants** en tant qu'utilisateurs peuvent faire un retour sur la manière dont ils perçoivent l'utilisation des équipements mobiles dans les diverses situations (en mode connecté ou non, en classe, hors classe, hors établissement) ; ce retour peut être effectué par exemple sous la forme d'enquêtes distribuées en établissement ; en école il est préférable que l'enseignant collecte lui-même les informations auprès des élèves,
  - les **parents** peuvent être associés à cette démarche en décrivant leur perception de l'utilisation de l'équipement mobile par les enfants,
  - les évaluations des applications sur la **plateforme de référencement** des ressources,
  - le **support matériel** : taux de panne et nature des pannes,
  - le **support logiciel** : identifiant/mot de passe invalide, incompatibilité d'une application,
  - le **relais en établissement ou en école** : nombre de sollicitations (par les élèves ou par les enseignants), type de problème (logiciel, matériel),
  - les **éditeurs d'applications** peuvent être impliqués en donnant un retour sur leur vision de l'utilisation de leurs applications dans l'école ou l'établissement.

20.2. Analyse des usages

L'analyse peut être réalisée à un niveau établissement ou école, académique ou national. Cela dépend de la portée souhaitée de l'observation des usages.

L'analyse consiste à considérer les éléments collectés pour déterminer des grands axes d'amélioration ou bien au contraire mettre en évidence des points forts.

Par exemple, les données collectées peuvent éclairer sur :

- un choix de certaines ressources mal éclairé qui pénalise les usages pédagogiques ;
- l'inadéquation entre les caractéristiques des équipements mobiles (capacités de traitement ou stockage notamment) et les ressources utilisées ;
- le choix des services utilisés par rapport aux besoins (messagerie, messagerie instantanée, réseaux sociaux…) ;
- une utilisation très faible de l'équipement mobile due à des facteurs comme le manque de ressources utiles ou le manque de formation ;
- un espace de stockage distant mal dimensionné par rapport aux usages ;
- une difficulté de pilotage ou d'organisation au sein de l'établissement.

20.3. Amélioration

L'analyse peut mettre en évidence plusieurs points utiles, par exemple :

- un changement de la formule de stockage distant pour rationaliser les coûts et s'aligner sur une réalité constatée ;
- une remise à plat des ressources (contenus, outils, services) utilisées dans l'établissement pour mieux répondre aux besoins pédagogiques des enseignants.

21. Gestion d'un projet mobilité

Comme évoqué tout au long des chapitres précédents, un projet de mobilité consiste à s'appuyer sur des solutions à la fois de type matériel (EIM, équipements pour classe mobile ou terminaux BYOD) et logiciel (ressources numériques, solutions de MxM et gestion de classe, portails captifs…) pour répondre à des besoins d'usages pédagogiques.

Il s'agit d'un projet de déploiement de solution informatique au sens traditionnel du terme. Ceci implique une phase de préparation (quels besoins ? quelles populations ? quelle organisation projet ?) et un déroulement cadencé en étapes (établissement de cahiers des charges, appel à candidature, sélection des fournisseurs, réception, validation et mise en œuvre des solutions).

La mise en place d'une solution de mobilité suppose l'adhésion de l'ensemble des acteurs impliqués et un pilotage coordonné par la maîtrise d'ouvrage.

Le projet a pour objectif de définir la solution, de sélectionner les fournisseurs et de déployer cette solution.

Ce chapitre donne des éléments pour des porteurs de projet qui souhaitent valider la démarche de mise en œuvre de leur projet. Dans le cas des projets BYOD, il est recommandé de se reporter au guide des projets BYOD/AVEC.

21.1. État des lieux

21.1.1. Capitaliser sur les résultats d'expérimentations

Un certain nombre d'expérimentations et de travaux ont été réalisées (ou sont en cours) quant à la mise en place de solution de mobilité par des collectivités locales en France.

Il est important de profiter des retours d'expérience associés à ces expérimentations afin de limiter le champ des possibles en affinant la nature des besoins qualifiés et en identifiant les solutions déjà opérationnelles.

Dans le cadre de ces expérimentations, des choix ont été faits (type des équipements mobiles, solutions de MxM / gestion de classe). Les résultats des expérimentations peuvent confirmer ou infirmer ces choix. Ces résultats, à rechercher sur le portail éduscol pour les communications nationales, ou auprès des académies pour l'accompagnement des établissements, doivent être considérés en début de projet.

21.1.2. Identifier l'écosystème existant

En amont du projet, il est également pertinent d'analyser l'environnement technique et réglementaire en instruisant les questions suivantes.

- Quelles sont les contraintes réglementaires et légales notamment en matière de protection des données à caractère personnel ?
- Y a-t-il déjà eu un travail d'analyse des besoins des utilisateurs et un recensement des exigences vis-à-vis de la solution de mobilité à mettre en œuvre ?
- Des ressources numériques ont-elles déjà été évaluées ?
- Les établissements du périmètre sont-ils équipés d'un réseau Wi-Fi ? Dans la négative, le projet devra prévoir un volet sur ce point. L'équipement des établissements est une phase qui peut être longue suivant le périmètre et les intervenants.
- Quelles sont les contraintes de sécurité (réglementaires, normatives…) ?
- Quels sont les moyens de projection déjà disponibles dans l'établissement ou l'école ?

- Quelles sont les parties prenantes sur les systèmes d'informations (infogérants, services informatiques académiques ou « locaux ») qu'il faudra impliquer dans le projet ?

21.2. Les grandes étapes

Il est impératif de suivre une démarche structurée de gestion de projet pour traiter l'ensemble des thématiques qui permettront au projet d'aboutir dans les délais validés par les parties prenantes. Le projet doit être maîtrisé et piloté.

Les grandes étapes à réaliser dans ce contexte sont les suivantes :

- identification de la maîtrise d'ouvrage ;
- élaboration de la stratégie de mise en œuvre ;
- analyse de faisabilité juridique du projet et de ses impacts[32] ;
- définition de la solution ;
- sélection des fournisseurs ;
- élaboration des conventions & chartes et protection des données à caractère personnel ;
- préparation du projet de déploiement ;
- déploiement pilote ;
- mise en exploitation de la solution (déploiement généralisé) et suivi opérationnel.

21.2.1. Identification de la maîtrise d'ouvrage

Une équipe doit avoir en charge le pilotage et la maîtrise du projet ; elle est responsable de la définition du besoin, des objectifs du projet, de l'identification des jalons et du budget consacré à ce projet.

21.2.2. Élaboration de la stratégie de mise en œuvre

Cette étape est déterminante dans la mesure où elle permet :

- d'arrêter une vision partagée de la solution de mobilité et de sa généralisation ;
- de construire un langage commun ;
- de préciser la composition du groupe de partenaires et leurs rôles respectifs ;
- de mettre en place une structure conjointe de pilotage, de définir les grands axes stratégiques du projet ;
- d'élaborer un plan d'actions en considération des enjeux liés au contexte local.

Sur la base des objectifs communs et des décisions prises, cette étape inclut des travaux d'évaluation de la faisabilité y compris juridique du projet.

- Quels sont les besoins qu'on souhaite couvrir ? À quels usages souhaite-t-on apporter une solution technique ? Existe-t-il des solutions couvrant ces besoins ?
- Quelle est l'enveloppe budgétaire nécessaire ? Quel type d'adhésion aux assurances type casse ou vol est retenu ?

Enfin il s'agira de déterminer les plans d'action à déclencher pour garantir la réussite du projet.

[32] Le délégué à la protection des données peut être consulté pour cette analyse comme tout au long de la mise en œuvre et de l'exploitation du projet.

La validation de ce cadre initial permet de fixer la base du projet sur laquelle seront lancés les travaux de mise en œuvre et de déploiement de la solution de mobilité.

21.2.3. Analyse de la faisabilité juridique du projet et de ses impacts

Le responsable de traitement doit également réaliser ou faire réaliser une analyse d'impact pour les traitements qui répondent à la définition des traitements soumis à ce type d'analyse. Si cette analyse aboutit à la conclusion que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque, le responsable de traitement **DEVRA** consulter la Cnil préalablement au déploiement du projet. Dans tous les cas, dès la définition du projet, le Délégué à la protection des données (DPD) **DOIT** y être associé pour s'assurer que le projet respecte l'ensemble des contraintes mis à la charge du responsable de traitement par le RGPD et la loi informatique, fichier et libertés.

Le responsable de traitement **DOIT** inscrire le(s) traitement(s) dans le registre de traitements.

21.2.4. Définition de la solution

Pour définir la solution, il convient de répondre aux questions suivantes (y compris dans le cas d'un projet BYOD s'appuyant sur une solution de MxM).

- Quelles sont les populations ciblées pour le déploiement de la solution (enseignants et élèves par niveau) ? Quels sont les établissements concernés ? Quel est le volume des équipements mobiles cibles ?
- Quelles sont les plates-formes technologiques en présence (type de systèmes d'exploitation et d'équipements mobiles) ?
- La politique de sécurité visée est-elle applicable sur les équipements mobiles retenus ?
- Les équipements mobiles retenus sont-ils compatibles avec les moyens de projection déjà disponibles ?
- L'impression de contenu depuis les équipements mobiles est-elle nécessaire et les équipements mobiles retenus offrent-ils cette capacité avec les moyens d'impression disponibles ?
- Quelles sont les ressources numériques répondant aux usages souhaités ? Ces ressources sont-elles disponibles (disponibilité des binaires d'installation) et correspondent-elles à mes contraintes techniques ? Sont-elles conformes aux standards d'accessibilité (ex : PDF/UA) ?
- Quels sont les besoins d'infrastructures nécessaires associés (déploiement de réseau Wi-Fi ou intégration au réseau existant, mise en place de serveur de gestion de contenu numérique…) ?
- Quelles sont les contraintes réglementaires à prendre en compte ? Quelles sont les normes (par exemple de sécurité) à respecter ?
- Quel est le calendrier prévisionnel de déploiement de la solution auprès des utilisateurs finaux ?

Sur la base des informations issues de l'état des lieux, de la définition de la stratégie du projet et de l'approfondissement apporté dans cette phase de définition de la solution, un cahier des charges répondant de façon la plus détaillée possible aux questions ci-dessus (caractérisation des exigences fonctionnelles et techniques, des contraintes non fonctionnelles) doit être établi pour lancer un appel d'offres auprès de fournisseurs.

Selon le périmètre du projet, il convient ou non de le lotir comme suit :

- lot d'équipement matériel : fourniture des équipements mobiles, des accessoires, prestations de préparation des équipements mobiles (et des conteneurs de classe mobile le cas échéant) ;
- lot d'équipement logiciel : fourniture de solution de gestion d'équipements mobiles, fourniture de ressources numériques, fourniture de solution de gestion de ressources numériques et prestations de service de gestion associées ;
- lots d'infrastructure : mise en place de réseau et de bornes Wi-Fi, hébergement et services de gestion de serveurs ;
- lot de prestation de support : centre d'appel de support.

21.2.5. Sélection des fournisseurs

Cette phase consiste à évaluer les réponses des soumissionnaires vis-à-vis du cahier des charges. Cette évaluation doit être réalisée sur la base d'une grille de critères reprenant les réponses détaillées aux exigences et contraintes formulées dans l'appel d'offres.

Au-delà de l'offre financière du soumissionnaire (qui doit permettre d'avoir une vision claire des coûts de mise en œuvre : frais d'acquisition de solution, charges de fonctionnement récurrentes), la qualité de sa réponse technique et ses références (expériences) sur des projets similaires sont des éléments prépondérants dans le choix.

Les fournisseurs sélectionnés **DOIVENT :**

- s'engager contractuellement à mettre en œuvre les mesures techniques et organisationnelles nécessaires pour assurer la protection des données à caractère personnel ;
- fournir les garanties de la mise en œuvre de ces mesures, dans le cadre des obligations mises à leur charge par le RGPD et les dispositions légales en vigueur ;
- s'engager à apporter une aide et assistance au responsable de traitement pour démontrer qu'il respecte ses propres obligations.

Les porteurs de projet **DOIVENT** inscrire les exigences de ces mesures dans leur cahier des charges et vérifier leur bonne exécution par des audits sur la durée du marché. Ces travaux se font en étroite collaboration avec les RSSI (Responsable de la sécurité des systèmes d'information) des académies, des collectivités territoriales et des prestataires.

21.2.6. Élaboration des conventions & chartes et protection des données à caractère personnel

Les porteurs de projet doivent formaliser le partenariat et les engagements respectifs des différentes parties prenantes, en particulier :

- la relation conventionnelle entre les partenaires du projet (collectivité territoriale, académie, établissements/écoles) ;
- les conditions de mise à disposition et d'utilisation des équipements par les élèves et leurs enseignants ;
- la remise de l'équipement aux élèves et enseignants, lorsqu'il s'agit de la mise à disposition d'EIM pouvant être rapportés au domicile ou bien de terminaux BYOD acquis par la collectivité et dont la propriété a été transférée aux familles.

La relation partenariale entre les parties **DOIT** être formalisée dans une convention de partenariat, décrivant ce que chacune des parties s'engage à faire vis-à-vis de l'autre, les éléments ayant contribué à la formation de la relation conventionnelle, les circonstances et intentions des parties ou encore les spécificités du contexte territorial. Les responsabilités en termes de protection des données **DOIVENT** être clairement définies.

Les clauses de protection des données conformes aux RGPD et la loi informatique, fichier et libertés modifiée en 2018 **DOIVENT** être intégrées dans les conventions.

La mise à disposition et l'utilisation des équipements aux utilisateurs **DOIVENT** être formalisées dans des documents décrivant la remise, les conditions de mise à disposition et d'utilisation (conventions de mise à disposition, bordereau de remise, chartes d'usages ou encore règlement intérieur).

Ce dispositif conventionnel **DOIT** notamment :

- informer de manière claire et compréhensible (en tenant compte du contexte et de leur âge) les personnes concernées par les traitements de données à caractère personnel dans le respect du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018 ;
- informer les utilisateurs de leurs responsabilités respectives, de la durée de la mise à disposition, des mesures de sécurité et modalités d'hébergement ;
- informer les responsables légaux des possibilités permettant d'assurer le contrôle des accès en dehors du temps scolaire (contrôle parental par exemple) ;
- préciser aux utilisateurs (élèves et enseignants) que la sauvegarde de leurs données privées leur incombe ;
- préciser aux enseignants, élèves et leurs responsables, le dispositif d'assistance et les modalités d'accès au support ;
- prendre les mesures nécessaires pour encadrer l'hébergement : la Cnil recommande dans la mesure du possible de mettre en œuvre des solutions permettant d'héberger les données dans des pays de l'Union Européenne ou assurant un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes ;
- préciser aux enseignants, élèves et leurs responsables les modalités d'activation de la géolocalisation de l'équipement mobile via le système de gestion de parc, en cas de vol ou de perte, lorsque le projet la prévoit.

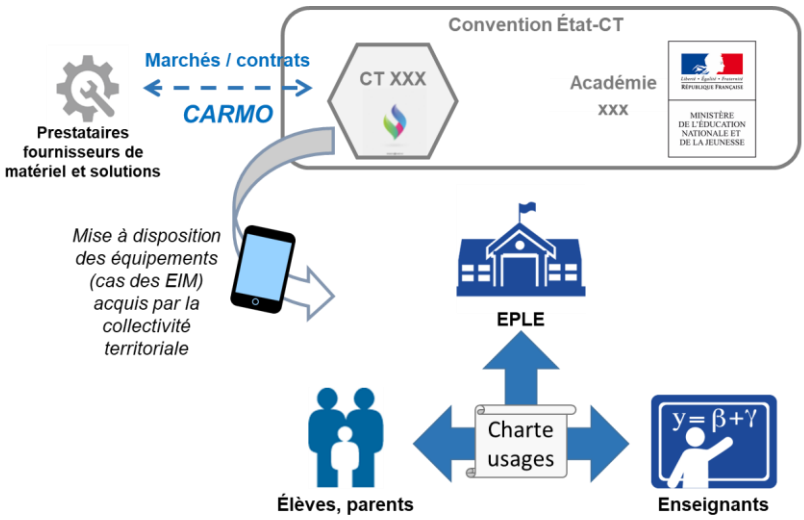


Illustration 26 : Représentation schématique des relations conventionnelles

Comme étape préalable au démarrage du projet en établissement, chaque responsable de traitement (chef d'établissement, ou inspecteur d'académie – directeur académique des services de l'éducation nationale) **DOIT** s'assurer que le projet d'équipements mobiles respecte les principes de protection dès la conception et tout au long du projet ainsi que le principe de protection par défaut.

Les porteurs de projet doivent accompagner les responsables de traitement dans l'exercice de cette responsabilité (documents d'accompagnement, de sensibilisation, éléments techniques et contractuels permettant de prouver que les prestataires retenus sont en conformité avec la loi…).

Les responsables de traitement doivent pouvoir démontrer que leurs traitements de données respectent les obligations qui leur sont imposées par le règlement européen de protection des données et la loi informatique, fichiers et libertés modifiée en 2018.

21.2.7. Préparation du projet de déploiement

Une fois le ou les différents prestataires retenus, une étape de lancement du projet doit permettre, sur la base des échéances calendaires du projet de valider un plan projet détaillé incluant :

- les principaux jalons à respecter, les dépendances entre lots du projet - par exemple, si on veut inclure dans la phase de préparation des équipements mobiles des applications mobiles, on doit s'assurer que celles-ci seront disponibles en entrée de la préparation des équipements mobiles ;
- les rôles et responsabilités des intervenants ;
- les livrables intermédiaires et finaux ;
- les comités de décision et de revue d'avancement ;
- les modes d'échange et de coordination des parties prenantes sur les différents lots du projet sont alors définis et validés.

En amont de la mise en exploitation de la solution, un responsable de la solution doit être désigné. Il a en charge de piloter le suivi opérationnel de la solution (voir ci-dessous « 21.2.9 - Mise en exploitation de la solution (déploiement généralisé) et suivi opérationnel »).

21.2.8. Déploiement pilote

Avant la mise en exploitation globalisée de la solution, il convient de mener une phase pilote qui correspond à la mise en production de l'ensemble de la solution (EIM ou terminaux BYOD, ressources numériques initiales, systèmes de gestion des équipements mobiles et des applications mobiles ou portail captif, composants d'infrastructure) sur un périmètre restreint d'utilisateurs.

Cette étape permettra une validation de bout en bout de la solution avant sa généralisation.

Durant cette étape, il est nécessaire de conduire une démarche d'accompagnement du changement, incluant la communication, la formation des utilisateurs, des équipes de supports, des administrateurs, ainsi que la diffusion de guides utilisateurs.

Une structure et une démarche d'évaluation sont également définies pour analyser l'impact de la mise en place de la solution de mobilité et tirer les enseignements nécessaires en vue de la poursuite de la généralisation et de l'évolution de la solution.

21.2.9. Mise en exploitation de la solution (déploiement généralisé) et suivi opérationnel

Après avoir évalué les résultats de la phase de déploiement pilote, en termes d'usages, de retour d'expérience, de remontée des demandes d'utilisateurs (pour lesquelles des arbitrages sont faits pour définir les évolutions fonctionnelles et techniques prioritaires), la solution de mobilité peut être généralisée à l'ensemble des écoles ou établissements cibles.

Au cours de cette phase se déroulent les services opérationnels (centre d'appel pour le support aux utilisateurs, service de gestion / maintenances des équipements mobiles, dont la distribution de nouvelles applications mobiles ou l'accès à de nouvelles ressources numériques). Pour les projets BYOD s'appuyant sur une solution de MxM, celle-ci peut prendre en charge la distribution de nouvelles applications mobiles.

Dans le cas des terminaux BYOD, la responsabilité de dommages causés à l'équipement reste limitée au cadre scolaire qui comprend le temps des activités scolaires (obligatoires ou facultatives), le temps de vie au sein de l'établissement et le temps des activités périscolaires.

Un responsable de la solution doit alors piloter les activités suivantes :

- suivi d'incidents (sur la base du pilotage de la cellule support et du compte rendu de ses interventions) avec les fournisseurs ;

- identification des violations de données et application, le cas échéant, de la procédure de notification des violations de données auprès de la Cnil, en accord avec les processus internes ;
- réalisation d'audit de l'application des règles de sécurité et d'habilitation ;
- analyse des retours d'expérience sur les usages, capitalisation sur les bonnes pratiques et identification des axes d'amélioration ;
- analyse de la prise en compte des élèves en situation de handicap ;
- veille préventive technologique ;
- vérification des possibilités de support et de périodes de garantie ;
- identification et priorisation des besoins d'évolution (par exemple évolution des politiques de sécurité) ;
- suivi budgétaire.

21.3. Organisation projet

Un chef de projet doit être désigné au sein de la maîtrise d'ouvrage pour piloter l'ensemble des phases du projet, du cadrage jusqu'à la recette du pilote. Pour la phase de déploiement généralisé et d'exploitation de la solution, le responsable de solution prend le relai du chef de projet (il peut s'agir de la même personne).

Le porteur de projet animera le comité de pilotage.

Si on prend en compte le périmètre le plus large d'un projet de mise à disposition de ressources numériques via un équipement mobile, le comité de pilotage doit notamment impliquer :

- des représentants des académies, des collectivités ;
- des représentants des utilisateurs pour travailler sur la caractérisation du besoin ;
- des représentants des équipes informatiques des collectivités locales concernées pour l'intégration avec des sous-systèmes du système d'information ;
- un responsable de la sécurité du système ;
- un responsable des achats pour la validation financière des offres des fournisseurs et la phase de contractualisation.

Ces représentants interviendront sur les choix stratégiques, le suivi de l'avancement projet, assureront l'arbitrage, la validation des travaux…

Le comité de projet avec des représentants des académies, des collectivités est à mettre en place pour gérer :

- la planification et la coordination des chantiers ;
- la prise de décisions pratiques ;
- le pilotage des intervenants ;
- le pilotage contrôle qualité ;
- la présentation des travaux au comité de pilotage ;
- le traitement des problèmes et la gestion des risques.

22. Conduite du changement

L'introduction d'équipement mobile dans une école ou un établissement représente un changement majeur dans la manière dont les enseignants et les élèves travaillent.

22.1. Adhésion des acteurs

Ce changement nécessite l'adhésion de tout un ensemble d'acteurs pour garantir le succès du projet :

- les utilisateurs - les élèves et les enseignants ;
- Les parents - bien que les parents ne soient pas des utilisateurs principaux des équipements mobiles, ils sont amenés à manipuler des EIM pour par exemple consulter le cahier de textes ou faire des révisions ;
- le personnel administratif.

L'adhésion s'obtiendra en communiquant sur les apports de l'équipement mobile dans l'établissement ou l'école. L'équipement mobile est un outil au service des usages pédagogiques, il les facilite.

La communication vise également à rassurer les parents sur la remise d'un EIM à leur enfant, sur l'utilisation qui en sera faite et les réponses que les parents peuvent se poser : mon enfant peut-il consulter les réseaux sociaux, jouer, aller sur internet…

Elle donne les informations pratiques utiles à l'utilisation de l'équipement.

Elle informe enfin sur la définition des responsabilités en cas de vol ou de détérioration et sur les droits des personnes au regard de la protection des données à caractère personnel conformément aux dispositions légales et réglementaires.

La communication peut être par exemple assurée :

- par un guide diffusé aux parents ;
- par une réunion d'information avant la remise des EIM.

Une fiche de mission pour le personnel encadrant les initiatives d'équipements mobiles permet de faciliter la prise en main et la maitrise de ce rôle.

22.2. Formation

L'équipement mobile nécessite un temps de prise en main, il doit être une aide et non une contrainte ou un frein aux usages. Une formation ciblée sur l'utilisation qui en sera faite est donc indispensable.

La formation peut prendre plusieurs formes :

- une formation initiale en début d'année pour une prise en main rapide et efficace ;
- une formation à la demande tout au long de l'année pour les utilisateurs qui le souhaitent ; cette formation peut être :
  - en ligne - un lien sur le bureau de l'équipement mobile qui pointe sur la formation peut être une réponse efficace,
  - en établissement - un ou plusieurs personnels relais peuvent avoir pour mission d'aider les élèves ou les enseignants en compléments des autres dispositifs de formations.

22.3. Suivi

Le succès du projet de dotation dans l'école ou l'établissement nécessite la mise en place de comités se réunissant de manière régulière pour suivre l'avancement du projet.

Ce suivi qui peut être mensuel peut aborder différents thèmes :

- la satisfaction et le retour des utilisateurs : ce point vient en complément de l'observation des usages discutée dans le chapitre 20 « Observation des usages » ; il permet d'être à l'écoute des utilisateurs qui sont les bénéficiaires du projet ;
- un état des lieux sur l'organisation dans l'école ou l'établissement ;
- un état des lieux sur la qualité des prestations acquises (stockage en nuage, outil de gestion de flotte…).

ANNEXES

A. Glossaire

Adresse MAC – MAC address

Une adresse MAC (Media Access Control), est un identifiant de réseau physique utilisé dans nombre de technologies réseau telles qu'Ethernet, Wi-Fi ou Bluetooth. À chaque fabriquant est affectée une (ou plusieurs) plage(s) d'adresses par l'IEEE (Institute of Electrical and Electronics Engineers). Un équipement mobile peut disposer de plusieurs interfaces réseaux et avoir ainsi plusieurs adresses MAC, par exemple une pour le Wi-Fi et une pour le Bluetooth.

Bien qu'il soit possible d'usurper une adresse MAC, les adresses MAC Wi-Fi peuvent être utilisées dans les processus de sécurité de premier niveau lors du raccordement au réseau de l'établissement ou de l'école puisqu'elles permettent de limiter le raccordement aux terminaux se présentant avec une adresse connue et dûment enregistrée.

AIPD (Analyse d'impact sur la protection des données)

L'analyse d'impact consiste en une analyse du risque concernant les répercussions potentielles du traitement de données prévu sur les droits et libertés des personnes concernées, tout en évaluant si les traitements sont susceptibles de présenter des risques spécifiques.

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

L'ANSSI a mission d'autorité nationale en matière de sécurité et de défense des systèmes d'information. Pour ce faire, elle déploie un large panel d'actions normatives et pratiques, depuis l'émission de règles et la vérification de leur application, jusqu'à la veille, l'alerte et la réaction rapide face aux cyberattaques — notamment sur les réseaux de l'État (ANSSI).

API (Application Programming Interface)

Une API désigne une interface applicative de programmation par laquelle un logiciel offre des services à d'autres logiciels.

BYOD (Bring Your Own Device)

LE BYOD « Bring Your Own Device » ou AVEC « Apportez Votre Équipement personnel de Communication » à l'École désigne l'usage, dans le cadre scolaire, d'un équipement numérique personnel dont la responsabilité ne relève ni de l'État ni de la collectivité.

Un équipement BYOD est un équipement numérique personnel dont la responsabilité ne relève ni de l'État ni de la Collectivité.

Cadre scolaire

Le cadre scolaire se définit comme le temps et le lieu où l'élève est placé sous la responsabilité de l'institution scolaire et où le règlement intérieur de l'EPLE, de l'école ou de l'internat s'applique.

Classe Mobile

Une solution classe mobile se compose a minima de plusieurs terminaux (dont un pour l'enseignant) et d'un conteneur sécurisé.

À la différence des EIM les terminaux d'une classe mobile ne sont pas affectés individuellement aux utilisateurs et ne quittent pas l'établissement ou l'école.

DPD

Il ressort du règlement européen sur la protection des données et des lignes directrices publiées par le G29, qu'il peut être défini comme la personne désignée, interne ou externe, en charge de veiller au respect de la règlementation relative à leur traitement par le responsable de traitement.

DoS (Denial of Service)

Une attaque par déni de service vise à rendre indisponible un service à ses utilisateurs en saturant les serveurs ou le réseau.

Débridage

Le débridage est un procédé permettant d'obtenir le contrôle total de l'équipement mobile.

EM (Équipement Mobile)

L'équipement mobile (EM) désigne un terminal informatique répondant à des besoins d'usages nomades.

EIM (Équipement Individuel Mobile)

L'équipement individuel mobile (EIM) désigne un équipement mobile affecté individuellement à un seul utilisateur et utilisable également en dehors du cadre scolaire.

ENT (Espace Numérique de Travail)

Un espace numérique de travail (ENT) désigne un ensemble intégré de services numériques choisis et mis à disposition de tous les acteurs de la communauté éducative de l'école ou de l'établissement scolaire dans un cadre de confiance. Il constitue un point d'entrée unifié permettant à l'utilisateur d'accéder, selon son profil et son niveau d'habilitation, à ses services et contenus numériques. Il offre un lieu d'échange et de collaboration entre ses usagers, et avec les autres communautés en relation avec l'école ou l'établissement.

Espace individuel

Espace dont l'usage est réservé à une personne. Des droits limités sur tout ou partie de cet espace peuvent être concédés à d'autres utilisateurs que le propriétaire, soit en vertu de règles organisationnelles écrites et connues de tous, soit par le propriétaire lui-même. Cet espace peut être visible d'un public plus ou moins étendu.

Espace personnel

Espace réservé à l'usage exclusif d'une personne et dont la confidentialité est garantie. Ne préjuge pas de l'usage principalement professionnel ou privé de l'espace.

Espace privé

Espace personnel réservé à des données considérées comme privées.

GPS (Global Positioning System)

Le GPS est un système de géolocalisation et navigation par un système de satellites qui permet localiser de manière très précise un équipement mobile, de l'ordre de quelques mètres.

LDAP (Lightweight Directory Access Protocol)

LDAP est un standard d'accès aux annuaires de l'IETF (LDAP).

MAM (Mobile Application Management)

On désigne par MAM les fonctions permettant de gérer l'administration et la délivrance d'applications mobiles pour un parc d'équipements mobiles.

Master

Un master est un ensemble d'applications mobiles dont la liste est définie pour une catégorie d'utilisateurs.

MCM (Mobile Content Management)

Le MCM est un ensemble de services et technologies qui fournissent un accès sécurisé aux contenus.

MDM (Mobile Device Management)

Une application de Mobile Device Management (MDM) ou "Gestion de Terminaux Mobiles", permet la gestion d'une flotte d'appareils mobiles. Cela peut aller d'une flotte d'une dizaine de terminaux identiques, jusqu'à des milliers de terminaux tous différents et tournant sous différents systèmes d'exploitation.

MxM

Appellation générique pour désigner indifféremment les fonctions de MDM, MAM, MCM.

MMS (Multimedia Message Service)

Le MMS est un système d'émission et de réception de messages multimédias (audio, photo, vidéo) pour la téléphonie mobile.

NFC (Near Field Communication)

Le NFC est une technologie d'échange d'informations à une faible distance, de quelques centimètres.

Over The Air (OTA)

Dans le contexte de cette étude OTA fait référence à la méthode de distribution d'une application mobile par le réseau sans fil. Cela permet depuis un emplacement central de mettre à jour tous les équipements mobiles des utilisateurs.

Profil

Un profil utilisateur est un ensemble d'informations concernant l'utilisateur, son (ses) rôle(s), ses préférences et le contexte dans lequel il se connecte qui peuvent être utiles pour la délivrance et le comportement du service.

QR Code (Quick Response Code)

Le QR Code (code à barres matriciel) est une évolution du code barre. Les informations sont codées en deux dimensions, sous forme de petits carrés noirs disposés dans un carré ou un rectangle sur fond blanc. Ils peuvent être lus par les équipements mobiles via l'appareil photo / caméra et décodés / interprétés par les applications pour des usages multiples.

Référentiel d'identité

Un référentiel d'identité désigne une base de données ou un annuaire rassemblant toutes les données d'identité d'une communauté d'individus et dans laquelle chacun est immatriculé de façon unique (cf. S2i2e – CARINE).

Ressources Numériques pour l'École (RNÉ)

Les ressources numériques pour l'École désignent les contenus et services associés (internes et externes à l'école ou établissement), créés, fournis et dimensionnés selon les besoins de la communauté éducative et la politique documentaire de l'établissement scolaire, en lien direct avec les textes de référence de l'Éducation nationale.

RFID (radio frequency identification)

L'identification par radiofréquences est une technologie permettant de stocker ou lire à distance des informations contenues sur une « radio étiquette », puce électronique incorporée à un objet et émettant ou répondant à des ondes radio. Selon la fréquence utilisée, la portée peut être de plusieurs mètres à quelques centimètres (*NFC*).

RGPD

Promulgué le 27 avril 2016, le Règlement européen de protection des données (RGPD) est entré en application le 25 mai 2018. Il a pour objet de mettre en place une protection homogène des données à caractère personnel et de favoriser les échanges au sein de l'Union européenne.

Rôle

Un rôle est un regroupement de tâches et d'accréditations qui concourent à la réalisation d'une ou plusieurs fonctions. Il détermine un ensemble d'actions qui peuvent être effectuées par la personne ou le groupe auquel il est affecté. Une personne (ou un groupe) peut se voir affecter plusieurs rôles. Un rôle peut, ou non, constituer un élément de profil vis-à-vis d'un service donné.

SD/Micro SD

Les formats SD et Micro SD sont des unités de stockage de petite taille pouvant être insérées sur un équipement mobile.

SMS (Short Message Service)

Ce service permet d'envoyer et de recevoir des messages alphanumériques depuis un équipement mobile.

SSO (Single Sign-On)

SSO signifie « authentification unique ». C'est une méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques ou sites web sécurisés.

Wi-Fi Direct

Le Wi-Fi Direct est une technologie définie par le Wi-Fi Alliance visant à améliorer les communications directes entre les équipements mobiles en Wi-Fi.

Source : IEEE Xplore

B. Exemple de grille de choix d'un équipement mobile

Voir le fichier « CARMO_Version_3_Annexe_B_grille_de_choix_équipement_mobile_*nnnnnn*.xls » joint en annexe.

Ce fichier propose un exemple de présentation et d'évaluation de critères pour aider à la décision de choix d'un équipement mobile, en complément des grilles de recommandations / exigences.

Le tableur est séparé en plusieurs catégories : caractéristiques matérielles, support matériel, préparation, accessoires.

Dans cet exemple, chaque équipement mobile en lice est évalué en regard des différents critères par une note de 0 à 5. Chaque note est pondérée selon l'importance accordée au critère.

Il peut être décidé qu'une note à 0 sur une pondération importante élimine de facto l'équipement mobile concerné.

> NB : dans l'exemple ici fourni, la pondération et le caractère éliminatoire des critères ont été positionnés de façon totalement arbitraire et ne reflètent en aucun cas une quelconque orientation ou jugement d'importance du MENJ. De même, la liste des critères retenus est proposée à titre indicatif. Il revient à chaque porteur de projet d'élaborer un système de notation reflétant les besoins et exigences de son projet.

Caractéristiques matérielles	Pondération de 1 à 3 (Importance)	Note EM1 (de 0 à 5)	Commentaire EM1	Note EM2 (de 0 à 5)	Commentaire EM2	Note EM3 (de 0 à 5)	Commentaire EM3	Note EM4 (de 0 à 5)	Commentaire EM4
Taille d'écran	2	0		1		1		5	
Qualité de l'écran	1	2		4		5		3	
Puissance	2	4		5		4		1	
Encombrement	2	1		3		0		5	
Poids	3	4		0		3		3	
Autonomie	3	3		1		2		5	
Stockage	2	3		5		3		5	
Communication (Wifi, ...)	3	2		2		1		3	
Connectique (USB, ...)	3	1		2		4		5	
Possibilité d'ajouter une carte mémoi	3	1		0		2		3	
EM résistant	2	2		0		1		4	
Prise en main	2	2		2		4		5	
	Total pondéré	59		51		67		110	
	Total sur 20	8,4		7,3		9,6		15,7	

Support matériel	Pondération de 1 à 3 (Importance)	Note EM1 (de 0 à 5)	Commentaire EM1	Note EM2 (de 0 à 5)	Commentaire EM2	Note EM3 (de 0 à 5)	Commentaire EM3	Note EM4 (de 0 à 5)	Commentaire EM4
Notoriété du prestataire	1	0		0		1		5	
Délais de réparation	3	2		4		5		3	
Procédure de livraison/restitution	2	4		5		4		1	
Ligne téléphonique dédiée	2	1		3		0		5	
Qualité de la gestion des incidents	3	4		0		3		3	
	Total pondéré	28		28		33		35	
	Total sur 20	10,2		10,2		12,0		12,7	

Accessoires	Pondération de 1 à 3 (Importance)	Note EM1 (de 0 à 5)	Commentaire EM1	Note EM2 (de 0 à 5)	Commentaire EM2	Note EM3 (de 0 à 5)	Commentaire EM3	Note EM4 (de 0 à 5)	Commentaire EM4
Clavier physique proposé	2	0		1		1		5	
Housse de protection proposée	1	2		4		5		3	
Diversité et qualité des accessoires	2	4		5		4		1	
	Total pondéré	10		16		15		15	
	Total sur 20	8,0		12,8		12,0		12,0	

Préparation	Pondération de 1 à 3 (Importance)	Note EM1 (de 0 à 5)	Commentaire EM1	Note EM2 (de 0 à 5)	Commentaire EM2	Note EM3 (de 0 à 5)	Commentaire EM3	Note EM4 (de 0 à 5)	Commentaire EM4
Mise en place de la housse de protection	2	0		1		1		0	Pas de préparation proposée
Temps de la préparation (respect des délais)	1	2		4		5		0	
Formatage et ajout d'une carte mémoire additionnelle	2	4		5		4		0	
Etiquettage des EM	3	1		3		0		0	
Installation de l'image	3	4		0		3		0	
Activation	5	3		1		2		0	
Finalisation	2	3		5		3		0	
Livraison	3	2		2		1		0	
	21								
	Total pondéré	52		46		43		éliminé	
	Total sur 20	9,9		8,8		8,2		0	

Synthèse	Pondération de 1 à 3 (Importance)	Note EM1	Commentaire EM1	Note EM2	Commentaire EM2	Note EM3	Commentaire EM3	Note EM4	Commentaire EM4
Caractéristiques matérielles	2	8,4		7,3		9,6		15,7	
Support matériel	1	10,2		10,2		12,0		12,7	
Accessoires	2	8,0		12,8		12,0		12,0	
Préparation	3	9,9		8,8		8,2		0,0	
	Total pondéré	72,8		76,6		79,7		éliminé	
	Classement	**2**		**3**		**1**		**ÉLIMINÉ**	

Illustration 27 : Exemples de grilles de choix d'un équipement mobile

C. Grille récapitulative des recommandations

La grille suivante est un récapitulatif de toutes les recommandations présentes dans le document. Elle permet une vue synthétique et peut être utilisée pour évaluer rapidement le niveau de réponse aux recommandations.

Équipement mobile – Caractéristiques matérielles

Id	Description	Prise en charge (non / partielle / totale)
#1.1	La taille de l'écran **DEVRAIT** être supérieure à 9 pouces	
#1.2	L'encombrement total de l'équipement mobile **DEVRAIT** respecter le format maximal 24x36 cm	
#1.3	L'équipement mobile **NE DEVRAIT PAS** dépasser une masse de 1,2 kg hors accessoires	
#1.4	L'équipement mobile **DOIT** offrir les services de connectivité suivants : Wi-Fi 802.11, Bluetooth (minimum 3.0)	
#1.5	L'équipement mobile **DOIT** pouvoir se connecter de manière sécurisée au réseau Wi-Fi de l'établissement	
#1.6	L'équipement mobile **PEUT** offrir la possibilité de diffuser des flux vidéo sur un vidéoprojecteur ou un écran externe	
#1.7	L'équipement mobile **DEVRAIT** offrir une autonomie suffisante pour une journée de cours, soit 8 heures	
#1.8	L'équipement mobile **PEUT** accueillir une mémoire externe, de type carte micro SD par exemple	
#1.9	La mémoire disponible **DEVRAIT** être au minimum de 32 Go pour l'utilisateur	
#1.10	L'enseignant et ses élèves **DEVRAIENT** posséder des équipements mobiles disposant du même système d'exploitation et des mêmes capacités de connexion	
#1.11	L'équipement mobile **DOIT** disposer d'une prise sortie audio et d'une entrée microphone, ou de Bluetooth (minimum 3.0). L'EIM **PEUT** proposer les deux solutions	
#1.12	L'équipement mobile **DOIT** disposer d'au moins une caméra. Le nombre de caméras et leur qualité **DOIVENT** être adaptés aux usages	
#1.13	L'équipement mobile **PEUT** disposer de connecteurs physiques permettant d'associer des périphériques (stockage externe, accessoires…)	

Tableau 10 : Récapitulatif des recommandations – Équipement mobile - Caractéristiques matérielles

Équipement mobile – Accessoires

Id	Description	Prise en charge (non / partielle / totale)
#2.1	Un clavier physique compatible avec l'équipement mobile **DEVRAIT** être associé à l'équipement mobile	
#2.2	Des claviers spécifiques **DOIVENT** être proposés pour des personnes en situation de handicap (plage braille, claviers alternatifs, claviers à suivi oculaire, claviers virtuels…)	
#2.3	Aucune fonctionnalité d'authentification de la dynamique de frappe au clavier **NE DOIT** être déployée	

Id	Description	Prise en charge (non / partielle / totale)
#2.4	Une housse ou une coque de protection **DOIT** être associée à l'équipement mobile si celui-ci n'est pas renforcé pour limiter les dommages	
#2.5	Un film protecteur **PEUT** être associé à l'équipement mobile	
#2.6	La housse de protection **DEVRAIT** permettre de mettre l'équipement mobile en position verticale ou inclinée et pas uniquement à plat	
#2.7	Des accessoires **PEUVENT** être associés à l'équipement mobile (stylet de pointage, stylet à pointe fine permettant d'écrire en posant la main, sondes techniques…)	
#2.8	Un dispositif d'écoute individuel (casque, écouteurs) **DOIT** être associé à l'équipement mobile	
#2.9	Les accessoires sélectionnés afin de compléter les équipements mobiles **DOIVENT** être adaptés afin de ne pas dégrader l'usage. Par exemple, veiller à ce que la housse de protection n'obture pas la caméra, le micro, les haut-parleurs, les prises de branchement, les boutons…	

Tableau 11 : Récapitulatif des recommandations – Équipement mobile - Accessoires

Préparation des équipements mobiles

Id	Description	Prise en charge (non / partielle / totale)
#3.1	Contractuellement, le prestataire **DOIT** être tenu d'assurer la sécurité et la confidentialité des données à caractère personnel auxquelles il pourrait avoir accès dans le cadre de ses prestations	
#3.2	Le prestataire **DOIT** placer la housse de protection	
#3.3	Le prestataire **DOIT** placer le film de protection de l'écran	
#3.4	Le prestataire **DOIT** insérer - et formater selon les cas - la carte mémoire additionnelle	
#3.5	Le prestataire **DEVRAIT** étiqueter les équipements mobiles	
#3.6	Les applications du socle d'applications **PEUVENT** être installées lors de la phase d'installation de l'image	
#3.7	Le prestataire **DOIT** automatiser toutes ces manipulations : installation des dernières mises à jour, du master établissement, du client MDM, configuration du Wi-Fi établissement, application des règles de sécurité	
#3.8	Le prestataire **DOIT** pouvoir récupérer les données des MDM/MAM	
#3.9	Le prestataire **DOIT** pouvoir lors de la préparation initiale de l'équipement mobile, y installer du contenu (audio, vidéo, PDF…) et lui associer le matériel Bluetooth (clavier)	
#3.10	Un système de livraison des terminaux (nouveaux équipements mobiles ou suite à une réparation) **DOIT** être mis en place	
#3.11	La charte utilisateur reprenant les règles à suivre **DOIT** être remise ou rappelée aux utilisateurs	
#3.12	La charte **PEUT** être distribuée lors de la mise à disposition de l'équipement mobile	
#3.13	La charte **PEUT** être sous forme numérique préchargée sur l'équipement mobile	
#3.14	Les engagements du prestataire **DOIVENT** être formalisés par le biais de contrat	

Tableau 12 : Récapitulatif des recommandations - Préparation des équipements mobiles

Support matériel

Id	Description	Prise en charge (non / partielle / totale)
#4.1	Une prestation de support matériel **DOIT** être proposée	
#4.2	L'image de l'équipement mobile hors terminaux BYOD (applications + données + paramètres de configuration) **DOIT** être sauvegardée, de manière sécurisée et dans le respect des dispositions légales et réglementaires en vigueur, pour remonter un équipement mobile à l'identique (opération de restauration)	
#4.3	Le prestataire **DOIT** fournir un état périodique des interventions de support qu'il réalise. Des indicateurs **DOIVENT** être définis	
#4.4	L'établissement ou l'école **PEUT** posséder un premier niveau de diagnostic de la panne, pour éviter de solliciter inutilement le support téléphonique	
#4.5	L'établissement ou l'école **DOIT** prévoir plusieurs équipements mobiles de remplacement	
#4.6	Des chargeurs supplémentaires **DOIVENT** également être disponibles pour les équipements mobiles qui ne sont pas rechargés	
#4.7	L'équipement mobile de remplacement **PEUT** être automatiquement configuré en fonction de l'utilisateur par récupération des paramètres et applications de l'utilisateur	
#4.8	Les élèves et les enseignants **DOIVENT** se voir proposer un numéro de téléphone et une plateforme d'assistance en ligne en cas de panne	
#4.9	Un contrôle des appelants **PEUT** exister afin d'éviter les appels sans rapport avec le support	
#4.10	Le support matériel **DOIT** être accessible sur une plage horaire définie et communiquée à l'ensemble des appelants potentiels	
#4.11	Les conditions de prise en charge des équipements mobiles pour réparation **DOIVENT** être précisées au moment de la remise de l'équipement (cf. §21.2.6 « Élaboration des conventions & chartes et protection des données à caractère personnel »). Les dispositions applicables pendant les vacances scolaires **DOIVENT** être mentionnées	
#4.12	Des colis de retour prêts à l'emploi **PEUVENT** être proposés par le prestataire du support	
#4.13	Le suivi **DOIT** être assuré avec par un exemple un numéro d'incident fourni à l'utilisateur ou l'établissement ou l'école	
#4.14	Un temps de prise en charge et de durée maximum de réparation **DOIT** être défini avec le prestataire en charge de la réparation	
#4.15	La sauvegarde des données pédagogiques **DEVRAIT** être automatique et transparente pour l'utilisateur	
#4.16	Une procédure de restauration **DOIT** être mise en place pour les données pédagogiques	
#4.17	Le projet **DOIT** prévoir des équipements mobiles de rechange à proposer aux élèves et enseignants pour compenser une indisponibilité de longue durée de leurs équipements mobiles, en particulier dans le cas des projets BYOD. Le projet **DEVRAIT** prévoir dans ce cas des équipements avec les systèmes d'exploitation les plus répandus afin d'éviter des problèmes d'incompatibilité des contenus et des applications	
#4.18	Le nombre d'équipements mobiles de réserve **NE DEVRAIT PAS** être inférieur à 2 % du nombre d'équipements mobiles du projet	

Tableau 13 : Récapitulatif des recommandations - Support matériel

Gestion des équipements mobiles (MDM)

Id	Description	Prise en charge (non / partielle / totale)
#5.1	Les équipements mobiles déployés **DOIVENT** pouvoir être inscrits grâce à la fonction MDM	
#5.2	La fonction MDM **DEVRAIT** pouvoir contrôler l'accès au paramétrage de l'équipement mobile	
#5.3	La fonction MDM **DEVRAIT** permettre d'interdire l'accès à certaines applications (par exemple le store)	
#5.4	La fonction MDM **DEVRAIT** pouvoir envoyer des notifications aux équipements mobiles	
#5.5	La fonction MDM **DOIT** pouvoir proposer la création de groupes d'équipements mobiles à usages différenciés	
#5.6	La fonction MDM **DOIT** pouvoir contrôler la façon dont les équipements mobiles sont sécurisés	
#5.7	Les systèmes d'exploitation (ROM) en cours d'utilisation sur les équipements mobiles **DOIVENT** être surveillés	
#5.8	La mise à jour des correctifs de sécurité du système d'exploitation **NE DOIT PAS** être automatique	
#5.9	Une fonction administrative de sécurité **PEUT** être proposée pour bloquer un équipement mobile	
#5.10	La fonction MDM **DOIT** pouvoir auditer les équipements mobiles. Le projet **DOIT** préciser les fonctionnalités précises attendues	
#5.11	Les administrateurs de la fonction MDM **PEUVENT** utiliser ses fonctionnalités pour réaliser des opérations associées à la sécurité sur les équipements mobiles	
#5.12	La fonction MDM **DOIT** pouvoir suivre le rythme des mises à jour des systèmes d'exploitation des équipements mobiles	
#5.13	La fonction MDM **DOIT** offrir un support en français	
#5.14	L'accès aux fonctionnalités et aux données de la fonction de MDM **DOIT** être sécurisé en conformité avec les recommandations en matière de sécurité de l'ANSSI et de la Cnil	
#5.15	La mise en place de la fonction MDM **NE DOIT PAS** entrainer un blocage des applications ou des configurations destinées aux élèves en situation de handicap	
#5.16	La compatibilité équipements mobiles / fonction MDM **DOIT** être vérifiée afin de bénéficier de la totalité des fonctionnalités du MDM, en particulier la version du système d'exploitation ou les personnalisations du constructeur	
#5.17	L'adresse MAC **NE DEVRAIT PAS** être utilisée par la fonction de MxM comme identifiant unique de l'équipement mobile (risque d'usurpation)	
#5.18	Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** s'assurer que les traitements de données mis en œuvre s'effectuent en conformité avec les dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018	
#5.19	La fonction MDM **DOIT** pouvoir s'interfacer avec le référentiel d'identité dans le respect des dispositions relatives à la protection des données et en particulier des principes de finalité, de proportionnalité et de minimisation	
#5.20	La fonction MDM **DOIT** pouvoir gérer l'ensemble des équipements mobiles de son périmètre	

Id	Description	Prise en charge (non / partielle / totale)
#5.21	La fonction MDM **DOIT** être capable de cloisonner de manière totalement étanche la gestion des équipements mobiles par structure organisationnelle	
#5.22	Une plage de service et de maintenance **DOIT** être définie	
#5.23	La disponibilité attendue durant la plage de service **DOIT** être définie	
#5.24	La solution technique retenue pour la fonction MDM **DOIT** être en phase avec la stratégie de déploiement et donc être évolutive pour prévoir la charge	
#5.25	La solution technique retenue pour la fonction MDM **DOIT** permettre la délégation de rôles aux établissements et écoles	
#5.26	La fonction MDM **DOIT** être à même d'interagir techniquement avec ses partenaires dans le respect des dispositions relatives à la protection des données et en particulier des principes de finalité, de proportionnalité et de minimisation des données	
#5.27	La fonction MDM **DOIT** pouvoir collecter automatiquement les informations auprès du référentiel d'identité ou **DOIT** être mise à jour par réplication	
#5.28	La fonction MDM **DEVRAIT** pouvoir mettre à disposition les informations nécessaires au prestataire responsable de la préparation de l'équipement mobile	

Tableau 14 : Récapitulatif des recommandations - Gestion des équipements mobiles (MDM)

Distribution des applications mobiles (MAM)

Id	Description	Prise en charge (non / partielle / totale)
#6.1	La fonction MAM **DOIT** permettre d'encadrer l'installation, la désinstallation et la mise à jour des applications	
#6.2	L'installation et la mise à jour d'applications **DOIT** pouvoir être faite par *OTA (Over The Air)*. La fonction MAM **DEVRAIT** dans ce cas permettre une optimisation des flux sur l'infrastructure locale	
#6.3	L'installation et la mise à jour d'applications **PEUT** être réalisée en mode poussé (push) silencieux ou en mode tiré (pull) en fonction des choix du projet. La fonction MAM **DOIT** pouvoir réaliser la modalité choisie	
#6.4	La fonction MAM **DOIT** pouvoir affecter une application au niveau établissement ou école, au niveau groupe ou au niveau individuel	
#6.5	La fonction MAM **DEVRAIT** être informée des commandes passées sur les dispositifs d'acquisition d'applications	
#6.6	La fonction MAM **DOIT** pouvoir suivre le rythme des mises à jour des systèmes d'exploitation des équipements mobiles	
#6.7	La fonction MAM **DOIT** offrir un support en français	
#6.8	Pour prévenir tout acte de malveillance, l'accès aux fonctionnalités et aux données de la fonction MAM **DOIT** être sécurisé	
#6.9	Les enseignants **DOIVENT** être impliqués dans la composition du portefeuille applicatif	
#6.10	L'accès au store applicatif associé au système d'exploitation **DOIT** être autorisé pour les enseignants afin de maximiser la découverte de nouvelles applications	
#6.11	Les informations concernant le délai de mise à disposition d'une nouvelle application **DOIVENT** être partagées avec les utilisateurs afin qu'ils puissent anticiper leurs demandes	

Id	Description	Prise en charge (non / partielle / totale)
#6.12	Un processus organisationnel permettant de regrouper les demandes et de s'assurer qu'elles sont traitées dans des délais raisonnables par les administrateurs **DEVRAIT** être mis en œuvre	
#6.13	Si l'affectation est réalisée dans un dispositif autre que le MAM alors les informations d'affectation **DOIVENT** être remontées dans le MAM	
#6.14	Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** s'assurer que les traitements de données mis en œuvre s'effectuent en conformité avec les dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018	
#6.15	La fonction MAM **DOIT** pouvoir s'interfacer avec le référentiel d'identité	
#6.16	La fonction MAM **DOIT** pouvoir gérer l'ensemble des équipements mobiles de son périmètre	
#6.17	La fonction MAM **DOIT** en conséquence être capable de cloisonner de manière totalement étanche la mise à disposition des ressources par structure organisationnelle	
#6.18	La fonction MAM **DEVRAIT** s'intégrer fortement avec la fonction MDM	
#6.19	Une plage de service et de maintenance **DOIT** être définie	
#6.20	La disponibilité attendue durant la plage de service **DOIT** être définie	
#6.21	La fonction MAM **DOIT** être à même d'interagir techniquement avec la technologie du référentiel d'identité	
#6.22	La fonction MAM **DOIT** permettre la délégation de rôles aux établissements et écoles	
#6.23	La fonction MAM **DEVRAIT** s'intégrer fortement avec la plateforme d'acquisition d'applications	
#6.24	La fonction MAM **DEVRAIT** s'appuyer sur la même gestion des groupes que le MDM	

Tableau 15 : Récapitulatif des recommandations - Distribution des applications mobiles (MAM)

Sécurité

Id	Description	Prise en charge (non / partielle / totale)
#7.1	Les acteurs d'un projet de déploiement d'équipements mobiles **DOIVENT** mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque	
#7.2	Des mécanismes de protection (filtrage…) **DOIVENT** être mis en place dans le cadre scolaire[33] (hors de ce cadre, il revient aux responsables légaux d'assurer le contrôle de ces accès)	
#7.3	Les objectifs de sécurité concernant les équipements mobiles **DOIVENT** être intégrés dans la politique de sécurité informatique de l'établissement	
#7.4	La fonction WPS (Wi-Fi Protected Setup) des points d'accès **DOIT** être systématiquement désactivée	
#7.5	Le code du réseau Wi-Fi **NE DOIT PAS** être divulgué	

[33] Cadre scolaire : voir glossaire

Id	Description	Prise en charge (non / partielle / totale)
#7.6	L'installation par l'utilisateur d'un système d'exploitation (ROM) alternatif **DEVRAIT** être interdite hormis pour les projets sans recours à la gestion de parc d'équipements BYOD	
#7.7	Les systèmes d'exploitation (ROM) en cours de déploiement **DOIVENT** être surveillés depuis la fonction MDM y compris pour les projets avec recours à la gestion de parc d'équipements BYOD	
#7.8	Un contrôle aléatoire des équipements mobiles **DEVRAIT** être mis en place	
#7.9	L'éditeur **DOIT** spécifier les prérequis matériels (et autres incompatibilités) de ses ressources	
#7.10	L'académie et les collectivités **DOIVENT** définir ensemble le panier minimum d'applications (en impliquant les enseignants)	
#7.11	Le matériel **DOIT** être choisi en fonction des ressources prévues	
#7.12	Les ressources choisies **DOIVENT** être supportées par le matériel	
#7.13	Les masters **DOIVENT** être compatibles avec le matériel (puissance requise et place totale occupée sur l'équipement mobile)	
#7.14	L'image (applications + données + configuration) de l'équipement mobile à l'exception des équipements BYOD non gérés par un outil de gestion de parc (MxM) **DOIT** être sauvegardée pour remonter un équipement mobile à l'identique (restauration)	
#7.15	Les données de l'espace pédagogique **DOIVENT** être sauvegardées de manière sécurisée et dans le respect des dispositions légales et réglementaires en vigueur	
#7.16	Les données de l'espace privé **NE DOIVENT PAS** être sauvegardées (la charte fera mention de cette exclusion)	
#7.17	L'équipement mobile **DEVRAIT** pouvoir être géolocalisé, dans le respect des dispositions légales et réglementaires, suite à une déclaration officielle de perte ou de vol effectuée par les responsables légaux et dans le cas d'une réquisition judiciaire	
#7.18	Des notifications **PEUVENT** être envoyées sur les équipements mobiles perdus ou volés	
#7.19	L'équipement mobile **DOIT** pouvoir être bloqué à distance. Cela vaut aussi pour les projets avec recours à la gestion de parc d'équipements BYOD	
#7.20	Les données de configuration (compte, Wi-Fi…) **PEUVENT** être supprimées à distance	
#7.21	Le système d'exploitation de l'équipement mobile **DOIT** être maintenu en permanence à jour des correctifs de sécurité	
#7.22	Des solutions d'analyse des usages des ressources, du trafic réseau…**PEUVENT** être mises en place dans le respect des obligations légales et réglementaires	
#7.23	Un antivirus **DEVRAIT** être installé sur l'équipement mobile dès la phase de préparation	
#7.24	La fonction géolocalisation de l'équipement mobile **DOIT** apparaître visiblement lorsqu'elle est activée et son activation **DOIT** recueillir le consentement de l'utilisateur	
#7.25	Tout accès par une application à la liste de contacts de l'utilisateur **DOIT** recueillir le consentement de ce dernier	
#7.26	L'EIM **DEVRAIT** être équipé d'un outil de contrôle parental avec un paramétrage par défaut. Le code d'accès au paramétrage est fourni aux parents.	
#7.27	L'EIM **DOIT** comporter un espace pédagogique	

Id	Description	Prise en charge (non / partielle / totale)
#7.28	L'EIM **DOIT** comporter un espace privé pour les données privées	
#7.29	L'espace personnel **DOIT** être défini (exemple : emplacement, limites) et nommé sans ambigüité (ex PERSONNEL). Des processus d'effacement irréversible des données **DOIVENT** être prévus pour chaque cas d'usage (changement d'utilisateur, fin de la durée de conservation prévue des données…). Les fichiers structurés de données à caractère personnel **DOIVENT** être stockés dans des espaces qui respectent la réglementation	
#7.30	L'accès à l'espace personnel d'un utilisateur **DOIT** lui être réservé, à l'exclusion de toute autre personne. Sans possession des moyens d'authentification de l'utilisateur, les données **NE DOIVENT PAS** pouvoir être consultées / modifiées. En particulier, les administrateurs techniques des espaces de stockage gèrent la capacité des espaces mais **NE DOIVENT PAS** accéder au contenu de l'espace personnel (clairement identifié comme tel) sans l'accord de l'utilisateur ou d'une autorité judiciaire.	
#7.31	Sans possession des moyens d'authentification de l'utilisateur les données ne **DOIVENT PAS** pouvoir être consultées/modifiées	
#7.32	Un seuil d'alerte **DEVRAIT** être défini pour prévenir l'utilisateur. Un seuil par espace (pédagogique et privé) **PEUT** être défini	
#7.33	Les productions **DEVRAIENT** pouvoir être supprimées à distance	
#7.34	La solution MxM **DEVRAIT** pouvoir offrir la possibilité à l'utilisateur de supprimer ses données personnelles	
#7.35	La réinstallation du système d'exploitation par un utilisateur **DEVRAIT** être empêchée	
#7.36	L'accès aux systèmes d'installation des applications par profil (enseignant versus élève) **DOIT** être contrôlé	
#7.37	L'administrateur local de l'établissement ou de l'école **DOIT** pouvoir mettre à jour le store privé avec les applications achetées par l'établissement ou l'école	
#7.38	Les élèves et les enseignants **DOIVENT** pouvoir installer, désinstaller ou mettre à jour une application depuis un store privé	
#7.39	La fonction MAM **DEVRAIT** permettre d'interdire l'accès à certaines applications (par exemple store)	
#7.40	La solution MxM **DEVRAIT** pouvoir contrôler l'accès au paramétrage de l'équipement mobile y compris pour les projets avec recours à la gestion de parc d'équipements BYOD	
#7.41	La solution de distribution des applications mobiles **DOIT** proposer un service fiable et réactif	
#7.42	Les prérequis exposés au chapitre 14.3.4« Services d'infrastructure pour l'établissement » **DOIVENT** être mis en place dans le respect des dispositions légales et réglementaires	
#7.43	L'accès à l'équipement mobile **DOIT** être sécurisé par un mot de passe répondant aux recommandations notamment de l'ANSSI et de la Cnil	
#7.44	Un verrouillage du terminal avec une mise en veille sécurisée au bout d'une inactivité de quelques minutes **DOIT** être proposé	
#7.45	L'EIM (hors terminaux BYOD) **DEVRAIT** être protégé par l'identifiant de connexion/mot de passe du compte ENT	
#7.46	L'accès aux applications comportant des données personnelles sensibles ou confidentielles **DEVRAIT** être sécurisé	

Id	Description	Prise en charge (non / partielle / totale)
#7.47	Les applications pouvant être téléchargées sur l'équipement mobile **DEVRONT** respecter le principe de demande d'autorisation préalable de l'utilisateur avant d'accéder à ses fichiers	
#7.48	Le dispositif conventionnel **DOIT** préciser aux utilisateurs les conditions d'utilisation de l'équipement mobile.	
#7.49	Une charte d'utilisation **DOIT** être mise en place et partagée	
#7.50	Les éditeurs d'application **PEUVENT** proposer des applications respectant un mécanisme de *SSO*	
#7.51	Pour les traitements de données biométriques qui répondent aux conditions déterminées notamment par la Cnil, le responsable de traitement **DOIT**, avant tout déploiement, réaliser une analyse d'impact (AIPD) et recueillir d'une manière adaptée le consentement de la personne concernée. Ceci concerne, par exemple, la reconnaissance d'empreinte digitale ou faciale	
#7.52	En cas d'utilisation de moyens d'identification et authentification basés sur des données biométriques (images d'empreintes, images d'iris…), les terminaux **NE DOIVENT PAS** stocker en clair ces données et **NE DOIVENT PAS** les envoyer vers un système d'authentification extérieur sous cette forme. Ils **NE DEVRAIENT PAS** les envoyer, même chiffrées ou hachées, vers un système extérieur et les y stocker, sauf justification impérative à inscrire explicitement au registre des traitements	
#7.53	Seules les informations nécessaires au fonctionnement de la solution de MxM ou de gestion de classe **DOIVENT** être exploitées. Les principes légaux de proportionnalité, de finalité et de minimisation **DOIVENT** être respectés	
#7.54	Les solutions de MxM / gestion de classe **DOIVENT** offrir des mécanismes sécurisés (protocoles et formats d'échange) d'intégration avec des annuaires externes ; on retrouve souvent LDAP ou Active Directory	
#7.55	Les solutions de gestion de parc (MxM et/ou gestion de parc informatique) et les services de gestion de classe **PEUVENT** être alimentés à partir de référentiels d'identité préexistants, mais **NE DOIVENT** reprendre que les données strictement nécessaires à leurs fonctions	
#7.56	Pour mettre en œuvre l'alimentation à partir des sources décrites dans le chapitre 14.6.3 et à partir d'autres référentiels, les responsables de traitement **DOIVENT** s'assurer que : ▪ les destinataires et émetteurs du flux sont bien identifiés (fiches de traitement inscrites dans le registre des traitements du responsable de traitement) ▪ les personnes concernées ont été informées conformément aux dispositions légales et réglementaires de cette communication	

Tableau 16 : Récapitulatif des recommandations - Sécurité

Gestion des productions numériques (MCM)

Id	Description	Prise en charge (non / partielle / totale)
#8.1	La solution mise en œuvre **DOIT** prévoir un espace de stockage des productions numériques	
#8.2	La fonction de MCM **DOIT** permettre aux utilisateurs d'ajouter, de modifier et de supprimer des travaux qu'ils ont réalisés	
#8.3	Dans les cas où l'établissement ou l'école a décidé de permettre à l'élève d'utiliser l'équipement mobile dans un cadre privé (valable également dans le cas du BYOD), l'EIM **DOIT** comporter un espace individuel, privé, pour les données privées	

Id	Description	Prise en charge (non / partielle / totale)
#8.4	L'EIM **DOIT** comporter un espace spécifique dit « espace pédagogique » associé aux activités scolaires	
#8.5	Si un espace privé existe, il **DOIT** être défini en précisant son emplacement et ses limites	
#8.6	Les données privées de l'utilisateur **DOIVENT** être identifiées par les mots "PERSONNEL" ou "PRIVÉ" (nom de répertoire ou de fichier, en-tête de message…)	
#8.7	Des seuils d'alerte **DOIVENT** être définis pour informer l'utilisateur qu'il s'approche de la limite de son volume de stockage attribué et disponible	
#8.8	Un système de quotas **DOIT** être mis en œuvre par profil (élève/enseignant) pour éviter un dépassement des limites des serveurs de stockage et une éventuelle surfacturation des services	
#8.9	Les productions **DEVRAIENT** être accessibles depuis différents terminaux (équipement mobile, PC via *ENT* par exemple)	
#8.10	La solution retenue pour la fonction MCM **DEVRAIT** pouvoir s'interfacer au référentiel d'identité.	
#8.11	L'accès aux productions **DOIT** être contrôlé en lecture et en écriture pour respecter les droits d'accès	
#8.12	Les services de stockage **DOIVENT** utiliser un antivirus régulièrement mis à jour pour garantir la sécurité	
#8.13	Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** s'assurer que les traitements de données mis en œuvre s'effectuent en conformité avec les dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018	
#8.14	Une plage de service et de maintenance **DOIT** être définie	
#8.15	La disponibilité d'accès attendue durant la plage de service **DOIT** être définie avec un taux proche de 99 %	
#8.16	L'infogérance **DOIT** anticiper la montée en charge en rapport avec les phases de déploiement des équipements mobiles dans l'établissement ou l'école si le déploiement est progressif	
#8.17	Les données **DOIVENT** être sauvegardées	
#8.18	Des capacités de restauration de données **DOIVENT** être proposées dans le service	
#8.19	Un contrat d'hébergement en bonne et due forme **DOIT** être proposé pour encadrer la prestation	
#8.20	Le format des productions **DOIT** être utilisable quel que soit le terminal	
#8.21	Un utilisateur **DOIT** pouvoir disposer d'un temps raisonnable (par exemple 3 mois) pour récupérer ses productions numériques dans le cas d'un départ en cours d'année scolaire	

Tableau 17 : Récapitulatif des recommandations - Gestion des productions numériques (MCM)

Outil de gestion de classe

Id	Description	Prise en charge (non / partielle / totale)
#9.1	L'enseignant **DOIT** pouvoir diffuser une ressource aux élèves de sa classe	

Id	Description	Prise en charge (non / partielle / totale)
#9.2	L'enseignant **DOIT** pouvoir autoriser, restreindre ou bloquer temporairement les accès à internet des élèves, en fonction des objectifs pédagogiques de la séquence	
#9.3	L'enseignant **DEVRAIT** pouvoir visualiser sur son poste de travail ou équipement mobile l'écran de ses élèves. Ceci afin de s'assurer de l'avancement des travaux, d'identifier les élèves ayant besoin d'aide	
#9.4	L'enseignant **DEVRAIT** pouvoir diffuser l'écran de son poste de travail ou équipement mobile sur l'écran des équipements mobiles de ses élèves	
#9.5	L'enseignant **DEVRAIT** pouvoir bloquer à distance l'équipement mobile des élèves, afin d'éviter les distractions lorsque l'équipement mobile n'est pas utilisé en cours	
#9.6	L'enseignant **DOIT** pouvoir autoriser ou bloquer certaines applications, pour un travail particulier, ou lors d'un contrôle	
#9.7	L'enseignant **DEVRAIT** pouvoir consulter la liste des équipements mobiles de sa classe ainsi que leur état (batterie, connectivité) afin de s'assurer de leur disponibilité pour tous les élèves	
#9.8	L'enseignant **PEUT** créer des enquêtes anonymes ou pseudonymisées et consulter le résultat	
#9.9	L'enseignant **DEVRAIT** pouvoir créer des groupes virtuels	
#9.10	L'enseignant **PEUT** bloquer ou autoriser la copie de données depuis ou vers un périphérique de type carte SD ou clé USB	
#9.11	L'enseignant **PEUT** autoriser un élève à afficher ce qu'il fait sur l'écran des autres équipements mobiles de la classe ou d'un groupe	
#9.12	L'enseignant **PEUT** diffuser simultanément un fichier audio ou vidéo à tous les élèves ou à un groupe	
#9.13	L'enseignant **DEVRAIT** pouvoir en un clic assombrir l'écran des équipements mobiles des élèves pour capter leur attention	
#9.14	L'enseignant **PEUT** mettre en place des sessions de discussion	
#9.15	L'enseignant **DEVRAIT** pouvoir utiliser son micro pour parler à un élève ou un groupe	
#9.15	L'enseignant **DEVRAIT** pouvoir écouter ce que dit un élève dans son micro	
#9.16	L'enseignant **DEVRAIT** pouvoir, de façon simple, apporter des commentaires écrits enregistrables sur l'interface élève de l'équipement mobile	
#9.17	L'enseignant **DOIT** pouvoir collecter facilement un travail fait par les élèves (audio, vidéo ou document)	
#9.18	Les fonctionnalités de gestion de classe **NE DOIVENT PAS** être utilisées à des fins de mesure d'activité ou de capacités cognitives de l'élève en dehors d'un cadre expérimental et contractuel où les sous-traitants de la solution s'engagent sur l'hébergement et l'exploitation des données à des fins éducatives pédagogiques (valorisation des données)	
#9.19	L'ENT et l'EIM **DEVRAIENT** partager un espace de stockage qui **DOIT** être associé au profil de l'utilisateur dès son authentification	
#9.20	Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** s'assurer que les traitements de données mis en œuvre s'effectuent en conformité avec les dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018	

Id	Description	Prise en charge (non / partielle / totale)
#9.21	Les fonctionnalités de la solution de gestion de classe **DOIVENT** être simples d'emploi et efficaces	
#9.22	La solution de gestion de classe **DEVRAIT** également intégrer les autres matériels connectés (ex. : vidéoprojecteur, TBI)	
#9.23	Les enseignants **DOIVENT** avoir été formés (cours ou autoapprentissage) à la manipulation des outils	
#9.24	Dans le respect notamment des principes de finalité, de proportionnalité et de minimisation des données définis par le RGPD et la loi informatique, fichiers et libertés modifiée en 2018, la solution de gestion de classe **DOIT** être capable de s'intégrer au référentiel d'identité ou au référentiel utilisé par la solution de MxM	

Tableau 18 : Récapitulatif des recommandations - Outils de gestion de classe

Support logiciel

Id	Description	Prise en charge (non / partielle / totale)
#10.1	Un guichet d'assistance logicielle **DOIT** être mis à disposition des utilisateurs	
#10.2	Ce guichet **DOIT** a minima proposer une assistance téléphonique pour répondre aux sollicitations des enseignants, du personnel académique ou de la collectivité territoriale, ou encore des élèves et de leurs parents	
#10.3	Le guichet d'assistance **DOIT** également proposer un portail en ligne comprenant des tutoriels, une rubrique « questions fréquentes », ou encore une messagerie instantanée	
#10.4	Ce portail d'assistance **DEVRAIT** être positionné sur l'écran d'accueil de l'équipement mobile comme raccourci lors de la préparation de l'équipement mobile	
#10.5	Le formulaire de demande d'assistance, de forum ainsi que la rubrique « questions fréquentes » **DOIVENT** être accessibles en dehors des heures ouvrables	
#10.6	Un document de type « convention de mise à disposition et d'utilisation » **DEVRAIT** décrire les modalités d'accès au support	
#10.7	L'assistance téléphonique proposée par la collectivité, l'académie ou l'éditeur de la ressource **DOIT** être ouverte durant des horaires en cohérence avec les besoins des utilisateurs et s'exécuter dans un cadre contractuel conforme au RGPD et la loi informatique, fichiers et libertés modifiée en 2018 en assurant notamment la sécurité et la confidentialité des données	

Tableau 19 : Récapitulatif des recommandations - Support logiciel

Classes mobiles

Id	Description	Prise en charge (non / partielle / totale)
#11.1	La configuration des salles et des bâtiments **DOIT** être prise en compte lors de la sélection du conteneur afin d'assurer les déplacements requis par l'usage prévu	
#11.2	Le conteneur **DOIT** disposer d'un dispositif de rechargement électrique des équipements mobiles	

Id	Description	Prise en charge (non / partielle / totale)
#11.3	Si ce dispositif de rechargement électrique nécessite de relier les équipements mobiles au conteneur via des câbles, ceux-ci **DOIVENT** avoir une taille suffisante et non excessive	
#11.4	Le conteneur **DOIT** pouvoir être relié au courant électrique et au réseau même lorsqu'il est fermé et sécurisé	
#11.5	Le conteneur **DOIT** posséder l'équipement adéquat pour ranger les câbles extérieurs lors des déplacements	
#11.6	Le volume de rangement du conteneur **DOIT** prendre en compte le volume des accessoires disponibles	
#11.7	Pour l'usage en classe mobile, un accessoire **DEVRAIT** permettre de brancher deux casques en même temps sur un même équipement mobile	
#11.8	Dans le cas où l'établissement n'est pas équipé d'un Wi-Fi sédentaire, la classe mobile **DOIT** être équipée d'une borne Wi-Fi pour relayer le réseau (accessible depuis une prise RJ45)	
#11.9	La borne Wi-Fi utilisée avec une classe mobile **DOIT** pouvoir être activée ou désactivée facilement par l'enseignant (par exemple via un interrupteur)	
#11.10	Dans le cas où l'établissement n'est pas équipé d'un Wi-Fi sédentaire, une seconde borne amovible **PEUT** être ajoutée au dispositif	
#11.11	Le matériel et les applications disponibles dans le cadre d'une classe mobile **DEVRAIENT** être gérés via des solutions de MxM	
#11.12	Le déploiement de mises à jour et d'applications **DEVRAIT** être programmé en dehors des plages d'utilisation des terminaux de la classe mobile	
#11.13	L'enseignant **DEVRAIT** disposer d'un équipement dédié	
#11.14	Le responsable du traitement (chef d'établissement dans le second degré, ou inspecteur d'académie – directeur académique des services de l'éducation nationale pour le premier degré) **DOIT** s'assurer que les traitements de données mis en œuvre s'effectuent en conformité avec les dispositions du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018	
#11.15	Dans le cas où une utilisation des terminaux dans le cadre périscolaire est envisagée, une charte co-rédigée par le directeur d'école et le responsable de l'équipe d'animation **DEVRAIT** être mise en place	
#11.16	Le lieu de stockage de la classe mobile **DOIT** permettre le branchement électrique et l'accès au réseau	
#11.17	Les utilisateurs d'une classe mobile **DOIVENT** disposer d'un espace sécurisé de stockage externe au terminal permettant de stocker les productions des élèves et de les retrouver à chaque séance	

Tableau 20 : Récapitulatif des recommandations - Classes mobiles

Gestion d'un projet mobile

Id	Description	Prise en charge (non / partielle / totale)
#12.1	Les porteurs de projet **DOIVENT** prendre en compte dans leur cahier des charges les mesures de confidentialité et de sécurité (conformes aux dispositions de l'article 35 de la loi du 6 janvier 1978 modifiée), et vérifier leur bonne exécution sur la durée du marché. Ces travaux se font en étroite collaboration avec les RSSI en académie	

Id	Description	Prise en charge (non / partielle / totale)
#12.2	Si l'analyse d'impact aboutit à la conclusion que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque, le responsable de traitement **DEVRA** consulter la Cnil préalablement au déploiement du projet	
#12.3	Dès la définition du projet, le Délégué à la protection des données (DPD) **DOIT** y être associé pour s'assurer que le projet respecte l'ensemble des contraintes mis à la charge du responsable de traitement par le RGPD et la loi informatique, fichier et libertés	
#12.4	Le responsable de traitement **DOIT** inscrire le(s) traitement(s) dans le registre de traitements	
#12.5	Les fournisseurs sélectionnés **DOIVENT** : ▪ s'engager contractuellement à mettre en œuvre les mesures techniques et organisationnelles nécessaires pour assurer la protection des données à caractère personnel ▪ fournir les garanties de la mise en œuvre de ces mesures, dans le cadre des obligations mises à leur charge par le RGPD et les dispositions légales en vigueur ▪ s'engager à apporter une aide et assistance au responsable de traitement pour démontrer qu'il respecte ses propres obligations	
#12.6	Les porteurs de projet **DOIVENT** inscrire les exigences de ces mesures dans leur cahier des charges et vérifier leur bonne exécution par des audits sur la durée du marché. Ces travaux se font en étroite collaboration avec les RSSI (Responsable de la sécurité des systèmes d'information) en académie	
#12.7	La relation partenariale entre les parties (collectivité territoriale, académie, établissements/écoles) **DOIT** être formalisée dans une convention de partenariat	
#12.8	Les responsabilités en termes de protection des données **DOIVENT** être clairement définies. Les clauses de protection des données conformes aux RGPD et la loi informatique, fichier et libertés modifiée en 2018 **DOIVENT** être intégrées dans les conventions	
#12.9	La mise à disposition et l'utilisation des équipements aux utilisateurs **DOIVENT** être formalisées dans des documents décrivant la remise, les conditions de mise à disposition et d'utilisation (conventions de mise à disposition, bordereau de remise, chartes d'usages ou encore règlements intérieurs)	

Id	Description	Prise en charge (non / partielle / totale)
#12.10	Le dispositif conventionnel **DOIT** notamment : ▪ informer de manière claire et compréhensible (en tenant compte du contexte et de leur âge) les personnes concernées par les traitements de données à caractère personnel dans le respect du RGPD et de la loi informatique, fichiers et libertés modifiée en 2018 ▪ informer les personnes concernées par le traitement de leurs droits d'accès, de rectification et d'opposition au traitement des données qui les concernent ▪ informer les utilisateurs de leurs responsabilités respectives, de la durée de la mise à disposition, des mesures de sécurité et modalités d'hébergement ▪ informer les responsables légaux des possibilités permettant d'assurer le contrôle des accès en dehors du temps scolaire (contrôle parental par exemple) ▪ préciser aux utilisateurs (élèves et enseignants) que la sauvegarde de leurs données privées leur incombe ▪ préciser aux enseignants, élèves et leurs responsables, le dispositif d'assistance et les modalités d'accès au support ▪ le cas échéant, mentionner l'hébergement de données à caractère personnel dans un pays n'appartenant pas à l'Union européenne ▪ prendre les mesures nécessaires pour encadrer l'hébergement : la Cnil recommande dans la mesure du possible de mettre en œuvre des solutions permettant d'héberger les données dans des pays de l'Union Européenne ou assurant un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes ▪ préciser aux enseignants, élèves et leurs responsables les modalités d'activation de la géolocalisation de l'équipement mobile via le système de gestion de parc, en cas de vol ou de perte, lorsque le projet la prévoit	
#12.11	Comme étape préalable au démarrage du projet en établissement, chaque responsable de traitement (chef d'établissement, ou inspecteur d'académie – directeur académique des services de l'éducation nationale) **DOIT** s'assurer que le projet d'équipements mobiles respecte les principes de protection dès la conception et tout au long du projet ainsi que le principe de protection par défaut	

Tableau 21 : Récapitulatif des recommandations - Gestion d'un projet mobile

Fin du document