MyToutatice : Mettre du SelfData dans son ENT

Olivier Adam, Sophie Schaal, Annabel Bourdé, Albane Guihomat, Yannick Bré, Thierry Joffredo
Rectorat de l'académie de Rennes,
96 rue d'Antrain
35000 Rennes

Résumé

Les agents, élèves et parents disposent d'une offre de services numériques fournie par le ministère, l'académie, le lycée/collège et aussi les collectivités territoriales. Cette offre est fédérée dans un espace numérique de travail répondant au schéma directeur des ENT. Les utilisateurs réalisent leurs activités d'apprentissage et d'enseignement dans un nomadisme permanent : travail en établissement, dans les transports, à la maison, etc. Ils changent de classe, d'établissement, poursuivent leurs études. Différents équipements sont utilisés pour réaliser ces activités : ceux de l'établissement, ceux de la famille, les leurs... de nombreuses données sont dispersées…

Par ailleurs, le RGPD introduit le principe de la portabilité des données personnelles. Les utilisateurs de l'ENT doivent pouvoir les récupérer lorsqu'ils quittent leur établissement, quelle que soit leur dispersion dans différents services : cahier de texte, notes, applications d'e-learning, ...

Comment permettre aux utilisateurs de prendre le contrôle de leurs données selon le principe du SelfData ?

La région académique Bretagne a pour ambition de leurs fournir un espace numérique strictement personnel connecté à leur ENT Toutatice, compatible avec tout type de terminal, qui leur permette de récupérer leurs contenus dispersés dans des applications et de stocker leurs productions. Ainsi, les élèves et enseignants pourront accéder à leurs données année après année, assurer la continuité de leurs activités et, en quelque sorte confectionner leur portfolio[1]. L'intégralité des contenus de cet espace numérique personnel sera récupérable par son propriétaire à tout moment.

Cet article a pour objectif de présenter le besoin d'un espace numérique personnel qui soit propriété des personnes, le principe du self data, les solutions explorées, l'expérimentation avec la solution Cozy de la startup Cozy Cloud - une alternative française open source innovante et respectueuse de la vie privée - dans ses dimensions fonctionnelles et techniques.

1. Dossier personnel dans lequel les acquis de formation et les acquis de l'expérience d'une personne sont définis et démontrés en vue d'une reconnaissance par un établissement d'enseignement ou un employeur

Mots-clefs

Self data, rgpd, cloud, identité, oidc, oauth2, pims, ENP, Toutatice, Cozy Cloud

1 Contexte

1.1 La région académique Bretagne

La région académique Bretagne est une des dix-sept circonscriptions administratives de l'éducation nationale. Elle correspond exactement au territoire de la région Bretagne qui comprend quatre départements. L'académie est organisée en établissements d'enseignement scolaire comprenant les écoles, collèges et lycées, ainsi que des services administratifs, le rectorat et les directions des services départementaux de l'éducation nationale (DSDEN).

La région académique Bretagne est constituée d'un rectorat et de quatre DSDEN pour gérer l'administration de l'éducation sur le territoire. L'enseignement des élèves est réalisé dans 2 356 écoles, 384 collèges et 121 lycées. La communauté éducative comprend environ 10 000 agents administratifs, 43 000 enseignants pour 570 000 élèves scolarisés auxquels s'ajoutent les personnels techniciens et ouvriers de service (TOS) des collectivités et, évidement, les parents.

Le service public de l'éducation s'organise avec la participation des collectivités territoriales qui, suite aux successives lois de décentralisation, prennent en charge la gestion des bâtiments, des personnels TOS, des services de restauration et des activités périscolaires. Les écoles, collèges et lycées sont respectivement pris en charge par les communes, les départements et la région.

1.2 Un environnement numérique de confiance pour l'éducation

1.2.1 Partenariat avec les collectivités

Dans le domaine du numérique, les lois de décentralisation répartissent les compétences entre l'État et les collectivités. Ces dernières, depuis l'entrée en vigueur de la loi Peillon de 2013, ont responsabilité du financement et de la maintenance des équipements et services d'infrastructure au numérique des établissements dont elles ont la charge. Concrètement, cela concerne les domaines informatiques de gestion des équipements, de gestion des réseaux et systèmes, de stockage et de partage de contenus hébergés dans et hors de l'établissement scolaire (les serveurs de fichiers, les services de l'ENT, etc.).

Cette situation de partage de responsabilité avec de multiples institutions publiques, créé des disparités entre les établissements sur un même territoires académique.

Dans la région académique Bretagne, un partenariat est établi entre les collectivités et l'académie pour mettre en œuvre des environnements numériques selon un schéma directeur commun afin de garantir des usages numériques équitables sur l'ensemble du territoire breton.

C'est dans ce cadre que depuis 2007, l'académie assure le développement, l'intégration et l'hébergement de l'Espace Numérique de Travail (ENT) « Toutatice » ainsi que l'accompagnement pédagogique des enseignants et des élèves. L'ENT Toutatice est

l’espace numérique unique des acteurs et établissements de la communauté éducative bretonne.

1.2.2 L’ENT Toutatice

L’ENT Toutatice constitue une plateforme numérique offrant aux acteurs de la communauté éducative des applications, ressources et services en ligne liés à leur profil. Ces services numériques sont mis à disposition par plusieurs organismes publics : le ministère de l’éducation nationale et de la jeunesse, la région académie Bretagne, les établissements et les collectivités. Une fédération d’identité permet l’authentification unique des utilisateurs pour l’accès aux différentes offres de services de ces organismes. Un portail accueille les utilisateurs pour leurs présenter l’intégralité des applications et ressources numériques de ces offres de services, ainsi que pour leur permettre de collaborer et partager autour d’espaces de travail et d’espaces de publication. Les fonctionnalités de ce portail d’ENT ont été présentées aux JRES2013 [1].

Au regard des questions de protection des données personnelles, et plus particulièrement depuis l’entrée en vigueur du RGPD, cet environnement numérique constitue un cadre de confiance pour les agents et élèves des établissements de l’académie. Ce cadre, s’il protège les usages, ne permet pas toujours à l’élève et l’agent de conserver leurs données en fonction de ses mouvements dans le système éducatif.

1.3 De nouveaux besoins à satisfaire

L’environnement numérique de l’utilisateur ne suffit plus aujourd’hui. Les services de l’ENT sont accessibles sur le web mais peu intégrés aux équipements numériques d’aujourd’hui comme les portables, les tablettes, les smartphones. L’offre éducative actuelle manque d’applications de stockage en ligne et de partage de contenu pourtant nécessaires aux enseignants et élèves qui risquent par conséquent de se tourner vers des solutions de grands éditeurs comme les GAFAM[2].

1.3.1 Le nomadisme est devenu la norme

Les élèves et enseignants travaillent en classe, dans les transports, à la maison, depuis un équipement fourni par l’établissement scolaire, en utilisant le leur ou celui de leurs parents. Leurs données doivent être accessibles depuis n’importe quel équipement et depuis n’importe où.

Certains outils, comme ceux liés au stockage, ne sont souvent accessibles que depuis l’enceinte de l’établissement. À défaut de solutions de stockage en ligne confortables proposées par l’académie ou les collectivités, les enseignants nous disent utiliser à regret des solutions des GAFAM. Le constat est amer.

Comment proposer une alternative confortable et bien intégrée à notre environnement numérique de confiance et aux équipements des utilisateurs ?

1.3.2 Le travail collaboratif de plus en plus adopté

Les méthodes pédagogiques évoluent et requièrent davantage de travaux en groupe de la part des élèves, ponctuels ou sur plusieurs années comme les nouvelles modalités des épreuves du baccalauréat.

2. Les GAFAM désignent Google, Amazon, Facebook, Apple et Microsoft

L'environnement numérique de travail doit favoriser la mise en commun, la collaboration et le partage de documents.

Quelle solution permettrait cet échange de documents entre espaces personnels et leur édition en ligne, facilitant ainsi le travail en groupe, sur tous supports et quel que soit le lieu ?

1.3.3 Une portabilité des données d'apprentissage tout au long au long de la vie

L'écosystème Toutatice que nous proposons fournit de nombreux services numériques de différents éditeurs. Ces outils, organisés en silos, hébergent eux-mêmes les différentes données et les effacent pour la plupart à la fin d'une année scolaire. Les données des utilisateurs sont ainsi éparpillées dans de nombreux services qui peuvent être hébergés dans l'établissement scolaire, au niveau académique ou au niveau national.

Comment permettre aux utilisateurs de récupérer leurs données qui peuvent, par exemple, leur servir pour la constitution de leur portfolio ?

Lorsque les élèves quittent le système scolaire pour rentrer dans la vie active, pour poursuivre des études supérieures ou bien s'ils changent d'établissement voire d'académie, ils perdent leur accès à l'ENT Toutatice et donc à l'ensemble de données qui s'y rattachent. Il en est de même pour les agents.

Comment rendre transportables ces données tout au long du parcours de formation des élèves et de la vie professionnelle des agents ?

2 Le self data où comment éviter un drive de plus

Plutôt que de choisir une solution de drive classique opérée par l'institution, pourquoi ne pas centrer le besoin sur l'utilisateur et lui donner la maîtrise de son espace numérique personnel tout long de son parcours scolaire ou professionnel ?

Cet objectif séduisant a poussé nos recherches vers le concept de Self Data.

2.1 Le principe du Self Data

La FING – fondation internet nouvelle génération – porte ce concept de Self Data.

« le self data consiste en la production, l'exploitation et le partage des données personnelles par les individus, sous leur contrôle et à leurs propres fins. »

La FING en donne les principes suivants [2] :

1. Respecter la réglementation européenne ainsi que les législations nationales relatives à la protection des données personnelles et de la vie privée.
2. L'accès, l'ajout ou la récupération de données personnelles dans l'espace personnel sécurisé d'un utilisateur, l'installation et l'activation d'une application ou d'un service utilisant ces données, ainsi que le partage de données avec des tiers, ne peuvent intervenir que sur la base du consentement préalable, informé et explicite de l'utilisateur et sous son contrôle permanent.
3. Les utilisateurs des espaces personnels peuvent à tout moment corriger ou supprimer les données personnelles les concernant qui y sont inscrites.
4. Le stockage, l'utilisation et l'échange de données personnelles, ainsi que d'identités numériques, sont sécurisées au meilleur niveau de l'état de l'art. La conception des services et des applications respecte les principes du privacy by design[3].
5. Le Self Data vise à fournir aux individus la connaissance, le contrôle effectif et l'usage des données qui les concernent, pour développer leur auto-détermination informationnelle et leur pouvoir d'agir.
6. Les utilisateurs sont libres d'utiliser les données qu'ils ont fournies, transmises, produites, coproduites, collectées ou récupérées, selon ce qui fait sens pour eux.
7. Dans l'esprit du développement du droit à la portabilité, les utilisateurs disposent en permanence de la possibilité de récupérer toutes leurs données et contenus stockés dans leurs espaces personnels.

2.2 Le Self Data dans le contexte de l'Éducation

L'utilisateur : un élève ou agent qui produit, réunit, gère et exploite ses propres données personnelles à ses propres fins et sous son contrôle.

Le détenteur de données : les écoles, collèges et lycées, le rectorat, le ministère ou encore les collectivités détiennent des données personnelles à propos d'individus, qu'elles aient été captées (ex. traces), recueillies (ex. formulaires) ou coproduites (ex. transaction).

La plateforme : elle permet aux élèves et agents de réunir ses données personnelles (ou les autorisations d'accès à ses données via des API et autres connecteurs) dans un « espace numérique personnel » sécurisé, de les gérer et de les exploiter soit par ses propres moyens, soit à l'aide de services tiers.

3. Concept ayant pour objectif de garantir l'intégration de la protection de la vie privée dans les nouvelles applications technologiques et commerciales dès leur conception.

Les solutions de PIMS – Personal Information Management System – répondent à ce besoin.

Le réutilisateur, service tiers : il propose aux élèves et agents, qui choisissent de les utiliser, des services et applications qui s'appuient sur leurs données personnelles pour apporter une valeur d'usage.

2.3 Les plateformes du Self Data : Les PIMS

Les PIMS (Personal Information Management Systems) permettent le stockage des données personnelles des individus, leur administration, leur collecte et leur échange sous leur propre maîtrise. Elles servent d'intermédiaire entre les organisations, les individus voire même entre les individus et les services/applications tierces qui leur permettent d'exploiter leurs données. **Pour répondre aux enjeux décrits précédemment et aussi maîtriser techniquement l'architecture de PIMS, des solutions de Drive open source étaient imaginées. Pour autant, seules les solutions Cozy et SOLID se sont avérées en adéquation avec les principes du Self Data.** Ces deux solutions ont été finalement été évaluées.

2.3.1 SOLID

En 2018, Tim Berners-Lee crée la société INRUPT qui a pour objectif de mettre en oeuvre un PIMS basé sur le projet SOLID (social linked datastore) [3]. Il a pour objectif de fournir aux personnes un contrôle total sur l'utilisation de leurs données. Il propose de découpler les données et les applications qui créent et consomment ces données. Chaque personne crée son propre espace de stockage pour ses données, un « pod » (Personal Online Data store), et l'héberge où il le souhaite. Ce pod est comme un coffre fort numérique qui peut être ouvert pour que des applications tierces puissent accéder aux données en fonction des permissions accordées par l'utilisateur. Cette nouvelle façon de voir le traitement des données personnelles sur le web présente plusieurs avantages, le principal étant de donner à l'utilisateur un meilleur contrôle de ses données puisqu'elles ne sont plus stockées par une société mais dans un espace maîtrisé par l'utilisateur. Cette solution permet également aux entreprises qui créent ces applications d'éviter de gérer la synchronisation de données entre les services, l'export de ces données et le stockage en masse de données que cela peut impliquer.

Lorsque nous avons mené le travail d'analyse de cette phase exploratoire, cette solution n'en était qu'au stade de prototype inachevé et n'avait donc pas la maturité nécessaire pour couvrir nos besoins. Elle a donc été écartée dans le cadre de notre expérimentation. Cependant, elle s'avère très intéressante dans une approche de standardisation de la représentation des données des utilisateurs.

2.3.2 La solution Cozy

L'entreprise CozyCloud [4] propose une plateforme de « Cloud Personnel ». Chaque individu peut disposer d'un « Cozy », c'est à dire d'un serveur personnel avec sa propre base de données et son propre nom de domaine Internet. Le cozy présenté sur la figure 1 a un nom de domaine comprenant son identifiant, « olmada » en l'occurrence.

Description des fonctionnalités d'un Cozy grand public affichées sur la figure 1 :

– Fourniture d'un « drive », un espace de stockage strictement personnel, auquel il est possible d'accéder depuis un ordinateur comme un équipement mobile pour consulter, ajouter, modifier ou partager des contenus = « Cozy Drive ». Il peut être synchronisé sur un ordinateur au moyen d'une application de synchronisation ;

– Accès à un magasin d'applications outillant le cycle de vie des applications Cozy ;

– Interfaçage, à l'initiative de l'utilisateur, avec des fournisseurs de services et de contenus pour récupérer automatiquement dans son « Cozy Drive » les données qui lui sont mises à disposition aux travers de connecteurs. Un connecteur est un module applicatif qui s'installe dans un espace personnel et qui va récupérer les données personnelles détenues par un service par API ou « web scraping »[4] et les enregistre dans un dossier ;

– Fourniture d'applications utilisant les données collectées et conservées dans le « Cozy Drive ». Ces applications peuvent également mettre en relation des données d'origines diverses afin de leur ajouter de fortes valeurs d'usage au bénéfice de l'utilisateur. Par exemple, l'application « Cozy Bank » permet le rapatriement des relevés bancaires de plusieurs banques et l'agrégation de ces données afin d'obtenir un suivi personnalisé des dépenses d'un utilisateur ;

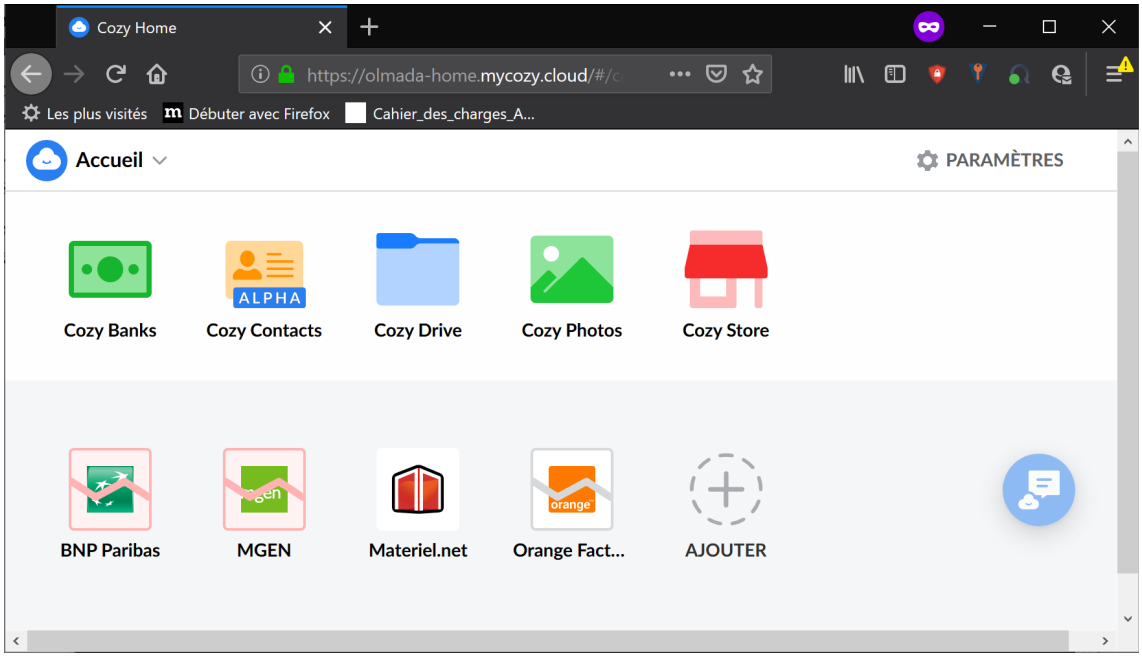

Figure 1 - Page d'accueil d'un cozy

L'hébergement des Cozy peut se faire de 3 façons :

– Mode SaaS (Software As A Service) permettant de démarrer le projet sans mettre en œuvre des composants d'infrastructure pour la phase d'expérimentation ;

– Hébergement sur infrastructures propres (par exemple : datacenter académique ou national) ;

– Hébergement personnel de l'utilisateur (par exemple sur un Raspberry Pi).

L'infrastructure de Cozy offre un protocole de partage en P2P pour que le partage et la synchronisation entre des hébergements sur des infrastructures distinctes soit transparente pour l'utilisateur ;

4. web scraping : technique d'extraction de données d'un site ou page html par un script ou un programme

Cozy Cloud mettra bientôt à disposition plusieurs applications intéressantes dans notre contexte :

- Application permettant de travailler directement depuis son espace numérique personnel pour créer des notes collaboratives intégrées au drive ;
- Application permettant l'édition de documents bureautiques de type traitement de texte ou tableur directement en ligne pour un travail personnel ou collaboratif ;
- Application « Cozy Agenda » permettant l'agrégation de plusieurs agendas ou calendriers qu'ils soient professionnels ou privés.

Enfin, la solution est open source et permet d'enrichir son offre par le développement de nouvelles applications et connecteurs.

3 Expérimentation : L’espace personnel MyToutatice

Ces recherches sur les principes et les solutions Self Data ont permis d’affiner notre objectif.

L’expérimentation mise en place a pour but de fournir un espace personnel sécurisé appelé « MyToutatice » aux élèves et agents de l’académie.

Cet espace MyToutatice permettra aux élèves de constituer, entre autres, leur portfolio avec les productions personnelles liées à leurs apprentissages et à leur orientation, leurs expériences et leurs compétences, en les partageant avec qui ils le souhaitent dans et hors de l’éducation nationale. Cet espace constituera un véritable lieu privatif d’auto-apprentissage de la gestion de ses données personnelles, de la protection du futur citoyen dans l’usage des services en ligne sur Internet : tout d'abord par la prise de conscience des données qu'il produit lui-même ou qui sont produites pour lui, et surtout par l'exploitation qu'il en fera à sa propre initiative et pour son propre bénéfice, dans le cadre d'une application de portfolio par exemple.

Elle permettra aux agents de développer les usages collaboratifs, mais également de conserver leurs données professionnelles dans leurs évolutions de carrière. Elle répondra aux témoignages récurrents d’un besoin de conservation et de réutilisation des documents administratifs très personnels : certifications (C2I2E, compétences, badges de compétence, PIX), arrêtés d’affectation, entretiens professionnels, salaires, ...

3.1 Écosystème de l’expérimentation

3.1.1 Choix de la solution partenaire : Cozy

Pour mener à bien cette première expérimentation, le choix s’est porté sur un partenariat avec l’entreprise Cozy Cloud et sa solution de « cloud personnel » Cozy.

La solution Cozy est un PIMS. Elle respecte donc les objectifs du Self Data.

Les fonctionnalités proposées de type « drive », les nombreux connecteurs et applications déjà disponibles, et la mise à disposition prochaine de note collaborative et d’édition en ligne des documents sont en adéquation avec les objectifs du projet d’espace personnel MyToutatice.

De plus, la documentation, l’accompagnement, la communauté et les licences open source de la solution Cozy permettent de prévoir des investissements dans le développement de nouveaux connecteurs et applications pouvant être intéressants pour les usages Éducation nationale.

3.1.2 Utilisateurs

Les élèves et agents du lycée Bertrand d’Argentré à Vitré ont été choisis comme premiers expérimentateurs de l’espace personnel MyToutatice.

Afin de passer rapidement à une expérimentation en lien direct avec le terrain et les retours utilisateurs, cet établissement bénéficie d’un espace MyToutatice avec une capacité de stockage de 5 Go par utilisateur depuis la fin de l’année scolaire 2018/2019.

3.1.3 Environnement Toutatice

La mise en œuvre d'un espace personnel MyToutatice s'appuyant sur la solution Cozy doit s'intégrer dans l'environnement technique de la région académique Bretagne, nommé pour la suite « l'environnement Toutatice » :

- L'ENT Toutatice : Point d'accès des utilisateurs à leurs services numériques éducatifs ;
- Hub d'identité ou Fédération d'identité Toutatice : Permet de fédérer les différents fournisseurs d'identité nationaux, académiques et territoriaux afin de fournir l'identité numérique éducative (ARENA pour les agents, EduConnect pour les élèves, etc.) à travers des protocoles SAML2, CAS et OpenId Connect. Le hub d'identité est présenté dans l'article « un HUB pour les fédérer tous » cette année aux JRES ;
- Annuaire « Toutatice » : Annuaire de type LDAP associé à l'ENT Toutatice et permettant, entre autres, la gestion des habilitations des utilisateurs ;

  L'environnement Toutatice est complété d'une plateforme « partenaires » permettant de reproduire un environnement complet (ENT Toutatice, LDAP, Fédération d'identité, APIs, etc.), ouvert sur l'extérieur. Toutes les données présentes sur cette plateforme sont représentatives des structures, de l'offre de services et de l'organisation académique. Les données d'identité sont préalablement anonymisées.

3.2 Description des travaux

Le partenariat avec l'entreprise Cozy Cloud nous a permis de mener à bien les travaux suivants :

- Adaptation de la solution Cozy au contexte de l'académie afin d'adapter les parcours utilisateurs pour la création et l'accès à leur espace MyToutatice en gardant l'ENT Toutatice comme point de départ pour les utilisateurs ;
- Accrochage de la solution Cozy à la fédération d'identité de Toutatice au moyen du protocole d'authentification OpenID Connect [5] afin de s'appuyer sur un standard d'échange sécurisé permettant le suivi des données transmises dans le respect du RGPD ;
- Exposition des données contacts « Éducation nationale » des utilisateurs à travers la mise en place d'une API sécurisée dans l'environnement Toutatice pour alimenter l'application "Mes contacts" de l'espace MyToutatice ;
- Développement et mise à disposition d'un connecteur ENSAP[5] par l'entreprise Cozy Cloud afin de permettre la récupération des bulletins de salaire dématérialisés des agents.

L'utilisation de la plateforme partenaires a permis de faire des tests de bout en bout entre l'environnement Cozy et l'environnement Toutatice dans des conditions similaires à l'environnement cible, ce qui a permis le passage rapide en production de la première version fournie au premier périmètre de l'expérimentation.

L'accrochage de la solution Cozy avec l'environnement Toutatice s'est faite dans l'esprit « privacy by design » recommandé par le RGPD, notamment en implémentant le consentement utilisateur, la validation des conditions générales d'utilisation (CGU) **claires et compréhensibles**, et l'accès aux données exclusivement par son propriétaire.

5. Espace Numérique Sécurisé de l'Agent Public

3.3 Parcours utilisateurs

3.3.1 Création de son espace MyToutatice

Afin de créer leur espace personnel MyToutatice, les élèves et agents à qui l'offre est proposée doivent se connecter à leur ENT Toutatice. Dans leur « bureau » de l'ENT Toutatice, un bouton leur est alors proposé afin de leur permettre de Créer leur espace MyToutatice en autonomie.

Figure 2 - Parcours utilisateur pour la création d'un espace personnel MyToutatice

Étapes de création :

– Les étapes 1 à 6 permettent la création de l'espace personnel MyToutatice à partir de l'identité numérique éducative de l'utilisateur de l'ENT. Cet utilisateur est informé des données personnelles transmises et, s'il le souhaite consent à la création de son espace après avoir pris connaissance des CGU. Il saisit alors un mot de passe propre à son espace MyToutatice afin, notamment, de pouvoir configurer les applications intégrées à ses terminaux.

– L’étape 7 propose à l’utilisateur de récupérer ses données de contact « Éducation nationale » à partir de l’environnement Toutatice afin d’alimenter l’application « Cozy Contacts » de son espace personnel. Il pourra ainsi utiliser ses contacts professionnels afin de partager des documents et collaborer.

– L’étape 8 est l’aboutissement de ce parcours. L’utilisateur peut alors utiliser pleinement son espace personnel MyToutatice.

–

–

3.3.2 Accès à son espace MyToutatice

Une fois leur espace MyToutatice créé, les élèves et agents voient, dans leur « bureau » de l’ENT Toutatice, un bouton leur proposant d’accéder à leur espace MyToutatice. Sur simple clic, ils peuvent alors y accéder sans ré-authentification.

Un agent dispose des fonctionnalités présentées dans la figure 3. L’application « Cozy Bank » est désactivée dans le cadre professionnel. Un connecteur est actuellement fourni pour permettre la récupération des bulletins de salaires détenus par l’ENSAP.

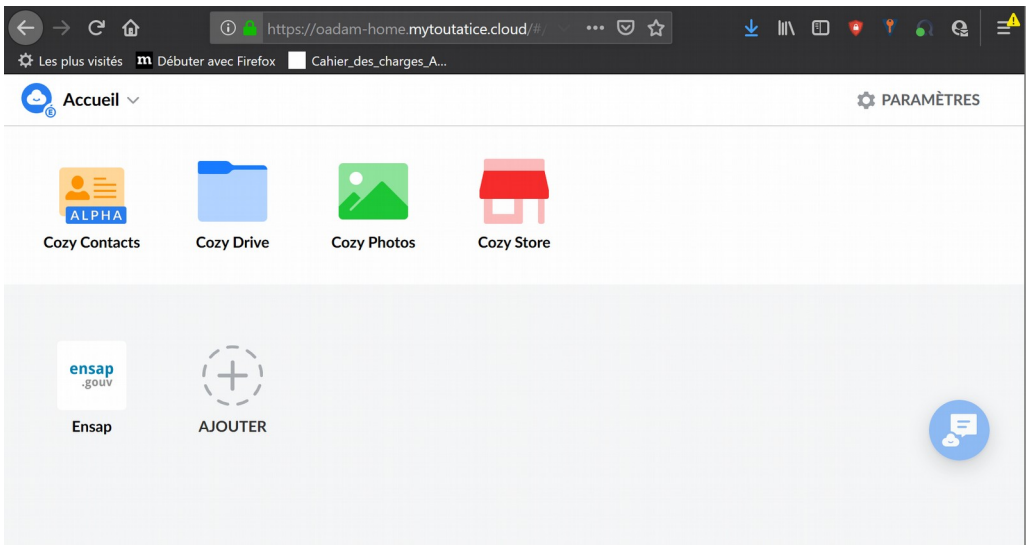

Figure 3 - MyToutatice d’un agent de l’académie

Dans le cas où l’agent configure un client sur son ordinateur (Linux, MacOS ou Windows), il accédera à ses données. La figure 4 présente le contenu du dossier contenant les bulletins de salaires automatiquement récupérés auprès de l’ENSAP et donc synchronisé sur son ordinateur.

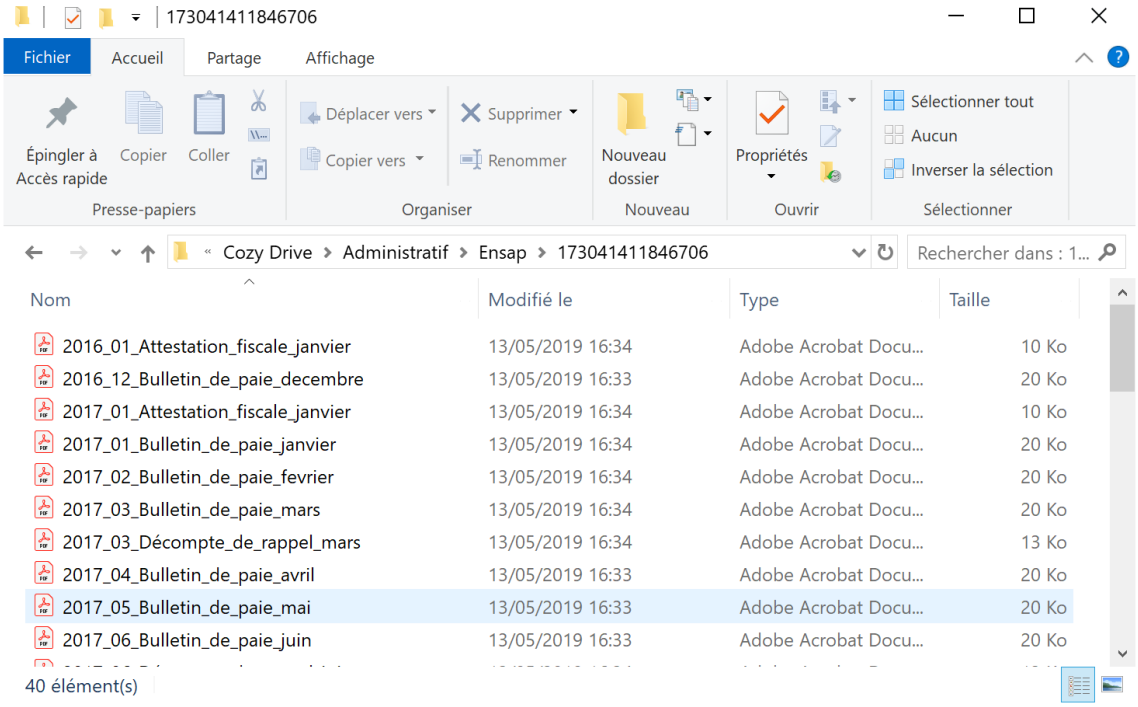

Figure 4 - Le dossier contenant les bulletins de salaire automatiquement collecté par le MyToutatice

3.4 Implémentation technique

3.4.1 Hébergement

Pour l'expérimentation, le choix s'est porté sur un hébergement chez Cozy Cloud.

Néanmoins, le domaine utilisé pour les URL des espaces MyToutatice (mytoutatice.cloud) a été acheté par l'académie de Rennes.

Pour la suite, une migration des espaces personnels existants et futurs est envisageable dans un environnement propriété de l'Éducation Nationale.

3.4.2 Connexion à la fédération d'identité de l'environnement Toutatice

Les travaux réalisés avec Cozy Cloud permettent donc à nos utilisateurs de créer un PIMS « MyToutatice » à partir de leur environnement Toutatice et de leur identité numérique éducative. Le mécanisme mis en œuvre est basé sur le standard OpenID Connect et le protocole OAuth2 [6]. Le principe est d'authentifier puis d'autoriser l'utilisateur pour l'accès à son espace personnel. Cozy Cloud a adapté sa solution Cozy afin de la rendre compatible avec ce protocole et a permis d'élargir le périmètre de confiance entre la fédération d'identité Toutatice et l'ENT Toutatice, aux espaces personnels MyToutatice créés.

L'utilisateur peut donc accéder à son MyToutatice à partir de son ENT sans ré-authentification. La figure 5 présente la séquence de ce parcours.

- L'utilisateur s'authentifie sur l'ENT Toutatice puis accède à son espace.
- La plateforme Cozy envoie une demande d'autorisation au serveur d'autorisation. L'utilisateur étant déjà authentifié dans la fédération d'identité Toutatice, le serveur d'autorisation renvoie un

access_token[6], un id_token[7] et un refresh_token[8]. Pour cette étape, l'« authorization code flow » d'OAuth2 a été mis en place.

– La plateforme Cozy requête ensuite le « endpoint userinfo » afin de récupérer le vecteur d'identité et permettre à l'utilisateur d'accéder à son espace personnel.

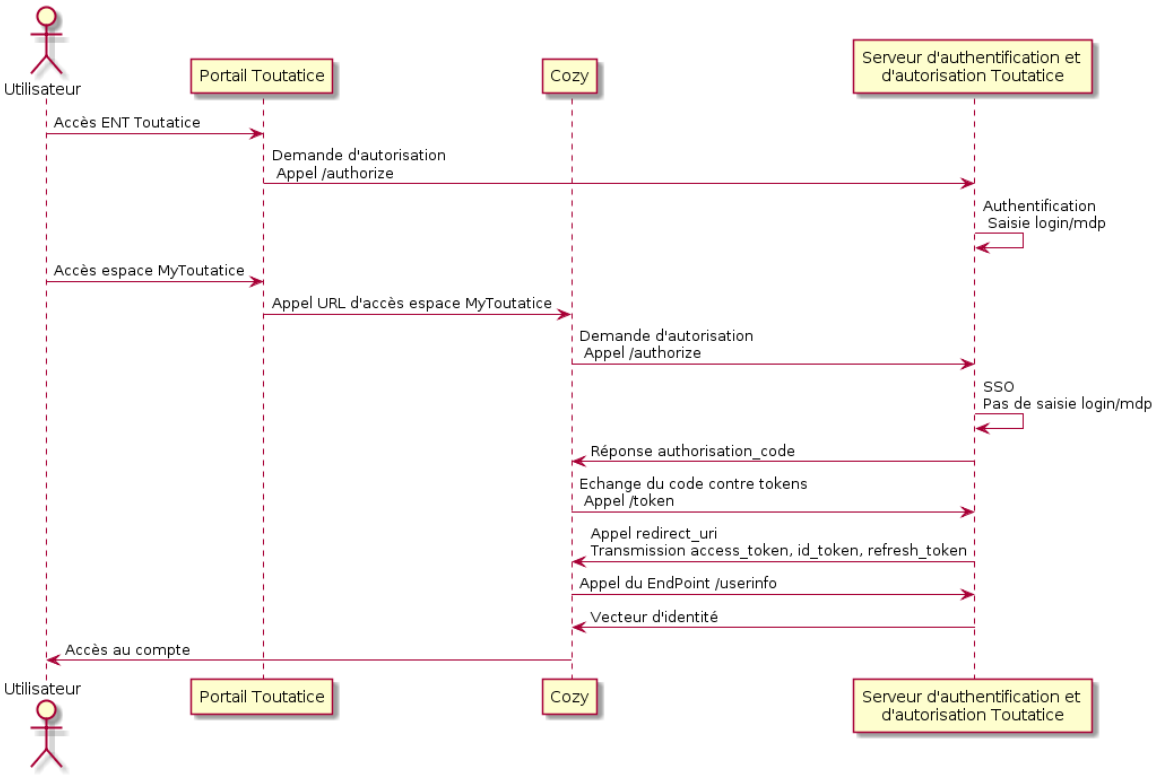

Figure 5 - Processus d'authentification de l'utilisateur à son espace personnel MyToutatice.

3.4.3 Création et accès à un espace personnel sécurisé

Les élèves et enseignants participant à la phase pilote de MyToutatice sont repérés dans l'annuaire Toutatice par un code offre :

– acrennes_cozy_exp_ele pour les élèves,

– acrennes_cozy_exp_ens pour les enseignants,

– acrennes_cozy_exp_pers pour les agents administratifs.

Le portail de l'ENT Toutatice se base sur la présence de ce code pour afficher une portlet[9] qui propose à l'utilisateur de créer son espace personnel. La figure 6 donne un aperçu de la portlet intégrée dans l'interface utilisateur. Lorsque la création est demandée, un identifiant est généré afin de permettre la définition de l'url d'accès à l'espace personnel. Par conception, chaque Cozy dispose de sa propre URL. Pour les espaces MyToutatice, les URL sont du type https://<identifiant>.mytoutatice.cloud.

6. Jeton d'accès
7. Jeton d'identification
8. Jeton de rafraîchissement
9. Portlet : module applicatif

L'identifiant doit donc être unique et compatible avec les conventions de nommage des noms Internet.

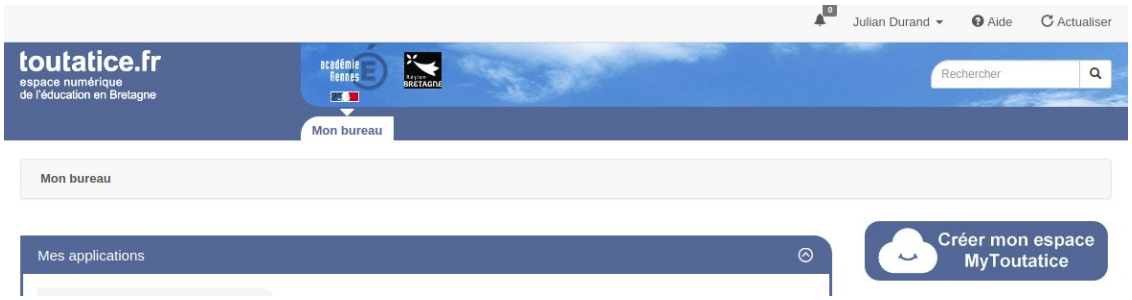

Figure 6 - Bureau Toutatice avec bouton de création d'un espace MyToutatice

A l'issue de la création de l'espace personnel, Cozy Cloud appelle l'API Feedback de Toutatice afin de confirmer la finalisation de la procédure de création et envoyer l'URL de l'espace généré. Cette URL est enregistrée dans l'annuaire Toutatice.

Lors de l'accès suivant de l'utilisateur à son ENT Toutatice, la portlet d'accès lui proposera d'accéder directement à son espace personnel, sans qu'il ait besoin de se ré-authentifier (figure 7).

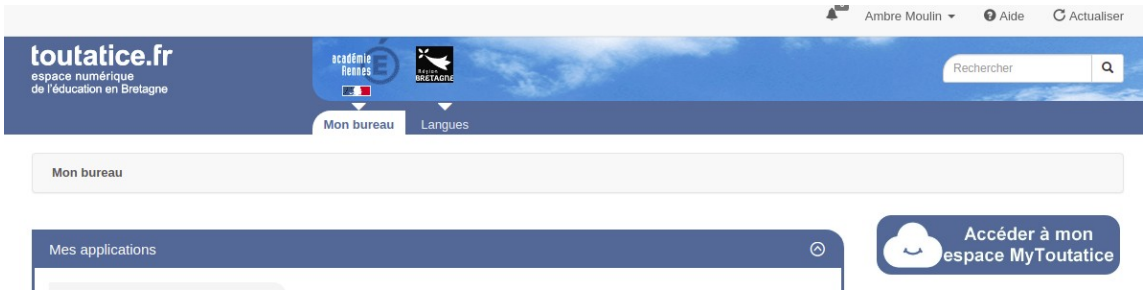

Figure 7 - Bureau Toutatice avec bouton d'accès à un espace MyToutatice

3.4.4 Collecte de données par API : Exemple des contacts « Éducation nationale »

Un exemple d'échange de données mis en œuvre dans cette expérimentation est la récupération des contacts « Éducation nationale » d'un utilisateur. La solution Cozy fournit déjà une application « Cozy Contacts » qui permet d'afficher les différents contacts importés dans l'espace personnel de l'utilisateur grâce à différents connecteurs (android, IOS, CardDAV, etc.).

Afin de fournir les données de l'environnement Toutatice permettant de définir les contacts professionnels d'un utilisateur, une API « Contacts » a été développée. Elle respecte les règles suivantes :

- Pour un élève, les contacts transmis sont les enseignants ainsi que les autres élèves de sa classe et de ses groupes.
- Pour un enseignant, les contacts sont les autres enseignants de ses établissements, ses élèves ainsi que des personnels en fonction des profils ENT des personnes.
- Pour un personnel, les contacts sont d'autres personnels récupérés en fonction des profils de l'ENT.

Pour répondre à ce besoin, l'entreprise Cozy Cloud a développé un connecteur consommateur de notre API. Les contacts sont alors stockés dans l'espace personnel de l'utilisateur. Ils sont affichés par l'application « Cozy Contacts » pour les gérer et aussi par « Cozy Drive » pour les activités de partage.

Afin d'assurer les échanges de données entre la solution Cozy et l'environnement Toutatice, une architecture basée sur des API sécurisées a été mise en œuvre. Cette architecture comprend des API exposées à l'extérieur et internes au système d'information de l'ENT Toutatice.

L'API « contacts » de l'environnement Toutatice est exposée à l'extérieur pour être interrogée par le connecteur contact côté espace personnel. Elle est protégée par le protocole d'autorisation OAuth2.

L'API contacts fait appel à une API interne qui est elle-même sécurisée via un token sous forme de bearer token présent dans l'en-tête HTTP Authorization de la requête. Ce token au format JWT [7] est pour le moment généré à partir d'un secret partagé entre les deux API. Ce mécanisme a vocation à évoluer pour utiliser un mécanisme OAuth2 (client credential flow) afin de supprimer ces secrets.

Cette architecture permet de faciliter la consommation de nos données par des tiers tout en garantissant une sécurisation en profondeur des données.

Les contacts chargés dans un espace MyToutatice sont intégrés dans des groupes permettant à l'utilisateur de se retrouver entre les différentes sources pouvant être utilisées. Les contacts créés manuellement dans un espace MyToutatice ne sont pas remontés dans l'environnement Toutatice qui reste alimenté par les différents SI de l'Éducation Nationale.

3.4.5 Interrogation manuelle de l'API contact

Lors d'une demande manuelle de mise à jour des contacts d'un utilisateur, la séquence d'autorisation présentée dans la figure 8 se déroule de la façon suivante :

- l'utilisateur, à partir de son espace personnel, fait une demande manuelle de récupération de ses contacts ;
- le connecteur fait appel à l'API Contacts avec un access_token valide sous forme de bearer token présent dans l'en-tête HTTP Authorization de la requête ;
- un contrôle d'accès basé sur le champ audience de l'access_token vérifie que l'appelant est autorisé à consommer cette API ;
- si l'appel à l'API est autorisé, l'API contacts fait appel à l'API interne avec un JWT sous forme de bearer token présent dans l'en-tête HTTP Authorization de la requête ;
- les données de contacts sont transmises au connecteur.

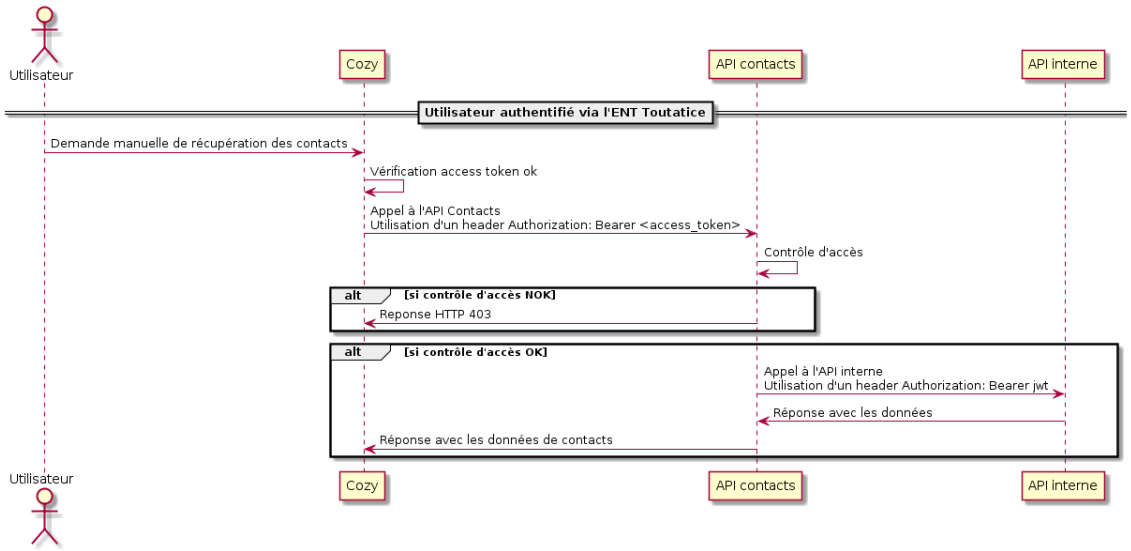

Figure 8 - Processus de récupération des contacts d'un utilisateur basé sur des API sécurisées.

3.4.6 Interrogation automatique de l'API contact

La mise à jour automatique et sans ré-authentification des contacts se fait avec le mécanisme OAuth2 dit de refresh_token. Il permet au connecteur d'obtenir un nouveau jeton d'accès (access_token) une fois que celui-ci a expiré. Il est stocké dans l'espace personnel de l'utilisateur. La figure 9 décrit ce fonctionnement.

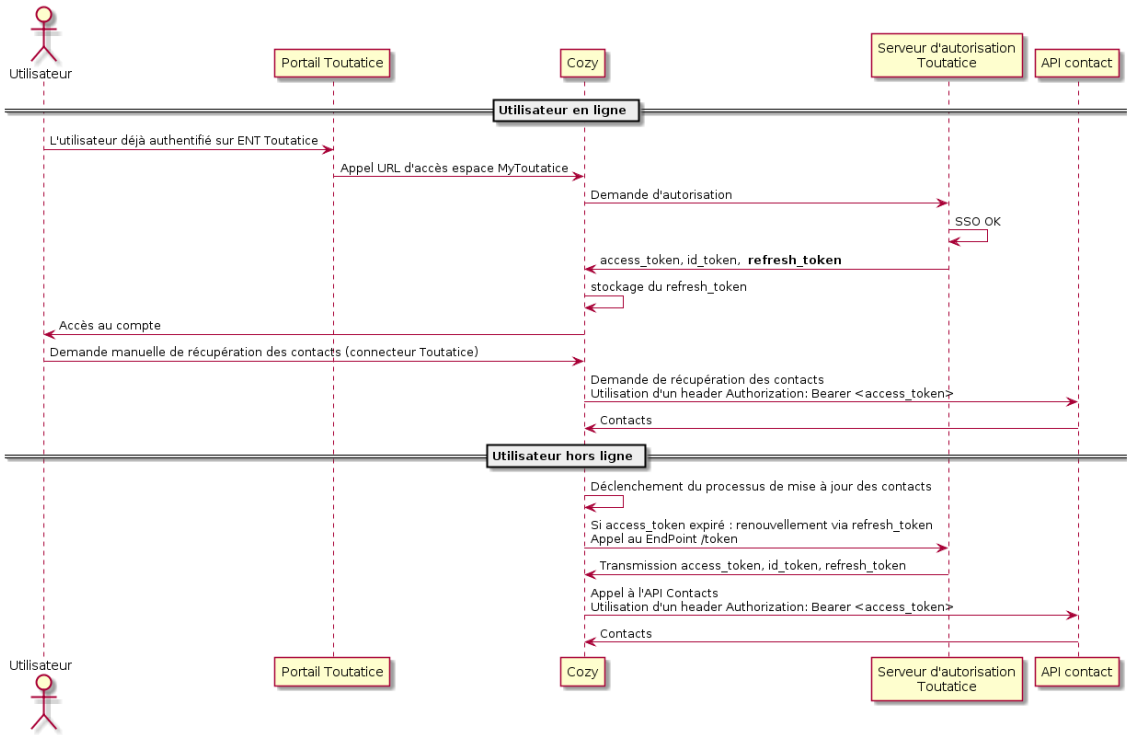

Figure 9 - Processus de récupération automatique des contacts via le refresh_token.

4

5 Maintenant et après

Les élèves et les agents peuvent bénéficier d'une solution d'espace personnel qui leur permettent de vivre leur mobilité, maîtriser leurs données et collaborer dans un cadre permettant le respect de la vie privée. Chaque propriétaire d'un MyToutatice est le seul à accéder à ses données. Pour un élève, il permet de constituer un cartable numérique réellement privé. Pour les agents et particulièrement les enseignants, il devient leur « espace professionnel personnel » fourni par l'employeur.

Au regard du droit de portabilité des données décrit dans le RGPD, les élèves et agents peuvent récupérer l'intégralité des données enregistrées dans leur MyToutatice. Il est prévu de leur permettre de le conserver après leur passage dans l'académie sous forme d'un Cozy de l'offre grand public de l'entreprise Cozy Cloud ou encore sur un hébergement de leur propre choix.

L'académie a pour ambition de développer cette solution pour répondre à des besoins éducatifs en se projetant dans l'hypothèse d'une généralisation qui ne pourra se faire sans se poser la question du modèle.

5.1 Quels besoins à couvrir ?

Nous avons pour objectif de fournir à nos utilisateurs une solution qui répondra au maximum à leurs attentes. Il est donc indispensable que nous retrouvions dans la solution proposée des services auxquels ils avaient déjà accès auparavant avec d'autres outils mais également de proposer de nouvelles fonctionnalités pour enrichir l'offre.

Dans cette perspective, de nouveaux connecteurs seront progressivement développés et mis à disposition des utilisateurs. Suivant la nature des connecteurs, ils seront présentés soit uniquement aux enseignants parce qu'ils sont en lien avec leurs activités professionnelles, soit à l'ensemble des utilisateurs.

Les connecteurs envisagés après échange avec les usagers sont :

- PMB : système de gestion documentaire du CDI (Centre de Documentation et d'Information) dans les établissements scolaires. Le connecteur permettra de collecter des traces telles que les notices documentaires des livres lus par élèves, les historiques d'emprunts effectués.
- Pronote : logiciel de vie scolaire présent dans de très nombreux établissements scolaires pour la gestion des notes, des emplois de temps, du cahier de textes, etc. Le connecteur permettra de rapatrier les données de l'élève comme les documents mis à disposition par l'enseignant (exercices, devoirs, corrections, ...), les bulletins, l'emploi du temps.
- Pix : service en ligne pour évaluer, développer et certifier les compétences numériques. Les données liées aux activités d'entraînement et de certification de l'utilisateur pourront être rapatriées.

D'autres connecteurs spécifiques aux personnels et aux enseignants seront également réalisés afin de rapatrier les données en lien avec les frais de déplacement des agents, les documents liés aux formations (attestation, ...), le dossier administratif des enseignants présent dans IProf (CV, arrêté d'affectation, ...).

Cette liste n'est pas exhaustive et sera amenée à évoluer en fonction des demandes des utilisateurs et des nouveaux services mis en œuvre.

Au-delà des connecteurs qui seront progressivement mis à disposition des utilisateurs, de nouvelles applications seront également intégrées aux espaces personnels :

- La note collaborative : l'utilisateur aura la possibilité de créer, modifier, partager une note collaborative intégrant du texte, des tableaux, des images, des sons, des vidéos et des liens. Elle pourra être enrichie collectivement en simultané par plusieurs utilisateurs après avoir été partagée.
- L'édition de documents bureautiques en ligne : sans que l'utilisateur n'ait à installer de suite bureautique sur son ordinateur, il pourra partager et éditer directement en ligne les documents de type traitement de texte, tableur et présentation (type diaporama). Comme pour la note collaborative, les différents documents bureautiques pourront être enrichis collectivement en simultanée par plusieurs utilisateurs après avoir été partagés. La solution OnlyOffice déjà utilisée dans les espaces collaboratifs sera utilisée.

Dans le rôle de réutilisateur du Self Data, des applications spécifiques au milieu scolaire seront intégrées au catalogue et proposées à tous les utilisateurs. Le tout, à initiative de l'utilisateur et à son unique bénéfice. Les applications ainsi envisagées :

- Calendrier / Agenda : Affichage d'informations provenant de différentes applications externes contenant ce type de données qu'elles soient "scolaires" ou "personnelles".
- Portfolio : À l'initiative de l'utilisateur, choisir et valoriser des données, ressources, documents ou travaux sélectionnés par l'utilisateur lui-même parmi les données présentes dans son espace numérique personnel.

5.2 Pour aller plus loin dans le Self Data

L’expérimentation actuelle positionne le PIMS comme un service périphérique de l’ENT. N’est-ce pas à cet espace personnel, de devenir le point d’entrée et de donner accès à l’intégralité de l’offre de services numériques éducation fédérée dans l’ENT ? Faire des espaces personnels MyToutatice le nouveau point d’entrée de l’élève et de l’agent sur leurs services est un objectif pour l’année 2020. Des travaux d’APIsation des catalogues des offres de services, portées par les différentes institutions, sont en cours au niveau de l’ENT Toutatice, afin de les rendre accessibles au sein de MyToutatice.

Par ailleurs, la réutilisation de données par des services tiers reste à démontrer. L’approche SOLID de Tim Berners-Lee avec le POD intéresse le partenariat Cozy Cloud / région académique Bretagne pour rendre accessibles les données collectées dans un standard.

Enfin, la solution actuelle est expérimentée en mode SaaS. Le passage à l’échelle questionne l’hébergement d’un tel dispositif pour une échelle académique voire nationale. La réversibilité des Cozy, actuellement hébergés par la société Cozy Cloud, pourra se faire sur autre hébergement. La solution Cozy, qui se défini comme un domicile numérique, a été conçue par défaut pour permettre ces déménagements. Pour autant, cette expérimentation pose la question d’une politique publique pour un espace numérique donnant au citoyen les moyens de maîtriser ses données. Qui, à terme, fourni et héberge ces PIMS connectés aux services publics en ligne de l’éducation, ainsi qu’à d’autres services ? L’individu, les collectivités, l’académie, l’état ? La question reste ouverte.

Bibliographie

[1] Toutatice, une plateforme Portail/ECM opensource pour la publication de contenus et de services métiers, JRES 2013 : https://2013.jres.org/archives/57/index.htm

[2] Charte du Self Data : http://mesinfos.fing.org/wp-content/uploads/2016/07/charte_selfdata.pdf

[3] https://solid.mit.edu/

[4] https://cozy.io/fr/

[5] OpenID Foundation. Specifications & Developer Information. http://openid.net/developers/specs/

[6] IETF OAuth 2.0. https://tools.ietf.org/html/rfc6749

[7] IETF JWT. https://tools.ietf.org/html/rfc7519