**Gestion des identités**

Référentiel des personnes & organisations

*Spécifications cible*

**Auteurs :**

 2020 –FusionDirectory

**Historique des révisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Révision** | **Date** | **Description** | **Auteur** |
| 1.0 |  | Réunion de lancement |  |
| 1.1 |  |  |  |
| 1.2 |  |  |  |
| 1.3 |  |  |  |
| 1.4 |  |  |  |

**Liste de distribution**

|  |  |  |
| --- | --- | --- |
| **Destinataire** | **Rôle – Organisation** | **Date** |
| Benoit MORTIER | Directeur FusionDirectory |  |
| Paola PENATI | Chef de Projet |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Liste d’approbation**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rôle** | **Nom** | **Organisation** | **Date** | **Signature** |
|  |  | Client |  |  |
|  |  | Client |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table des matières**

[1. OBJECTIF DE L’ETUDE 5](#__RefHeading___Toc5312_3407739022)

[1.1. Définition 5](#__RefHeading___Toc5314_3407739022)

[1.2. Critère d’éligibilité 5](#__RefHeading___Toc5316_3407739022)

[1.3. Méthodologie projet 5](#__RefHeading___Toc5318_3407739022)

[1.4. Equipe projet 5](#__RefHeading___Toc5320_3407739022)

[1.5. Espace projet 5](#__RefHeading___Toc5322_3407739022)

[2. ANALYSE DE L’EXISTANT 6](#__RefHeading___Toc5324_3407739022)

[2.1. Les référentiels actuels 6](#__RefHeading___Toc5326_3407739022)

[2.2. Les différentes populations 6](#__RefHeading___Toc5328_3407739022)

[2.3. Règles de gestion des comptes 7](#__RefHeading___Toc5330_3407739022)

[3. REFERENTIEL DE PERSONNES CIBLE 8](#__RefHeading___Toc5332_3407739022)

[3.1. Règle de gestion des données dans le référentiel 8](#__RefHeading___Toc5334_3407739022)

[3.2. Les données 8](#__RefHeading___Toc5336_3407739022)

[3.3. Les métadonnées 8](#__RefHeading___Toc5338_3407739022)

[3.4. Dotations et services fournis par catégorie de population 9](#__RefHeading___Toc5340_3407739022)

[3.5. Applications sources 11](#__RefHeading___Toc5342_3407739022)

[3.6. Applications consommatrices 12](#__RefHeading___Toc5344_3407739022)

[3.7. Le référentiel des organisations 12](#__RefHeading___Toc5346_3407739022)

[3.8. Les groupes 13](#__RefHeading___Toc5348_3407739022)

[4. La vision cartographie et process 14](#__RefHeading___Toc5350_3407739022)

[4.1. Création des comptes 14](#__RefHeading___Toc5352_3407739022)

[4.2. Authentification AD 14](#__RefHeading___Toc5354_3407739022)

[4.3. Transmission des informations vers le restaurant 14](#__RefHeading___Toc5356_3407739022)

[4.4. Génération du code lecteur Médiathèque 15](#__RefHeading___Toc5358_3407739022)

[4.5. Récupération des adresses mails étudiants 15](#__RefHeading___Toc5360_3407739022)

[4.6. Edition des badges et cartes étudiants 15](#__RefHeading___Toc5362_3407739022)

[4.7. Mise à jour et affichage de l’annuaire page blanche 15](#__RefHeading___Toc5364_3407739022)

[4.8. CVtheque 15](#__RefHeading___Toc5366_3407739022)

[4.9. Synchronisation avec le LMS Moodle 15](#__RefHeading___Toc5368_3407739022)

[4.10. Synchronisation avec Zimbra 15](#__RefHeading___Toc5370_3407739022)

[4.11. Récupération des mobilités de stage 15](#__RefHeading___Toc5372_3407739022)

[4.12. Affectation des droits dans l’ENT esup-portail 15](#__RefHeading___Toc5374_3407739022)

[4.13. Changement du mot de passe 15](#__RefHeading___Toc5376_3407739022)

[4.14. Droits d’accès à certaines ressources en salle de T.P. 15](#__RefHeading___Toc5378_3407739022)

[4.15. Accès au Helpdesk GLPI 16](#__RefHeading___Toc5380_3407739022)

[5. Architecture TECHNIQUE cible 17](#__RefHeading___Toc5382_3407739022)

[6. ASPECTS JuridiqueS : CNIL & DPO 18](#__RefHeading___Toc5384_3407739022)

[7. ANNEXE 1 : DETAILS DE LA METHODOLOGIE 19](#__RefHeading___Toc5386_3407739022)

[8. ANNEXE 2 : Définition des POPULATIONS 22](#__RefHeading___Toc5388_3407739022)

[9. ANNEXE 3 : Referentiels d’Organisation 24](#__RefHeading___Toc5390_3407739022)

[10. ANNEXE 4 : CARTOGRAPHIE APPLICATIVE 25](#__RefHeading___Toc5392_3407739022)

[11. ANNEXE 5 : Schéma OpEnLdap 26](#__RefHeading___Toc5394_3407739022)

# OBJECTIF DE L’ETUDE

## Définition

Un référentiel de personnes n’est pas un outil mais un ensemble de règles qui régit les données associées aux personnes.

## Critère d’éligibilité

Selon la DISI, les caractéristiques principales d'une donnée de référence sont donc le sens (la sémantique), la qualité, le partage et la réutilisation (en consultation principalement, et donc sans modification) par plusieurs acteurs et applications du système d'information. Cap Gémini fonde la définition des données de référence sur une approche **PIQR** répondant à 4 critères.

**Partage**.

**Identification**. Il s’agit de la définition sous forme syntaxique et sémantique de la donnée. Cela inclut également le processus de mise à jour et de propagation.

**Qualité**. Il s’agit de l’aptitude de l’ensemble des caractéristiques de ces données à satisfaire des exigences internes (pilotage, décision, sécurité, efficacité, efficience...) et des exigences externes (réglementation...) à l’organisation. Il s’agit bien du degré d’adéquation à l’usage que l’on en fait. Elle est mesurée par le delta d’interprétation par tous les utilisateurs métiers.

**Réutilisation** en respectant les 3 critères précédents.

## Méthodologie projet

L’annexe 1 décrit la méthodologie qui a été adoptée pour aborder ce projet.

## Equipe projet

L’équipe projet est transverse et regroupe à la fois les personnes de la DISI et les métiers notamment la RH et la COM interne.

En fonction de l’évolution, d’autres Directions métiers viendront se joindre au projet (formation, recherche…).

## Espace projet

Un espace projet a été créé.

Lien gitlab

# ANALYSE DE L’EXISTANT

L’analyse de l’existant montre qu’il n’existe pas un unique référentiel de personnes.

## Les référentiels actuels

## Les différentes populations

Un travail en commun avec la Direction des Ressources Humaines a permis de dénombrer un total de (nombre) **populations différentes au sens RH**.

|  |  |
| --- | --- |
| **Population** | **Volume** |
| Etudiants |  |
| Permanents en CDI |  |
| Personnels en CDD |  |
| Vacataires |  |
| Apprentis |  |
| Stagiaires |  |
| Doctorants contrat doctoral |  |
| Doctorants non payés |  |
| Post-Doc |  |
| Sabbatiques et Chercheurs invités |  |
| Personnels CNRS |  |
| Personnels associés ou invités |  |
| Professeurs émérites ou Maîtres de Conférence Honoraires |  |
| Incubés |  |
| Retraités |  |
| Extérieurs |  |

## Règles de gestion des comptes

Les règles de gestion listent les règles actuelles pour la **création et la suppression des comptes**.

|  |  |
| --- | --- |
| **Population** | **Règle en sortie** |
| Etudiants |  |
| Permanents en CDI |  |
| Personnels en CDD |  |
| Vacataires |  |
| Apprentis |  |
| Stagiaires |  |
| Doctorants contrat doctoral |  |
| Doctorants non payés |  |
| Post-Doc |  |
| Sabbatiques et Chercheurs invités |  |
| Personnels CNRS |  |
| Personnels associés ou invités |  |
| Professeurs émérites ou Maîtres de Conférence Honoraires |  |
| Incubés |  |
| Retraités |  |
| Extérieurs |  |
| Association / club |  |
| Syndicat |  |
| Système |  |

# REFERENTIEL DE PERSONNES CIBLE

Ce chapitre propose une cible pour le futur référentiel des personnes et les données associées.

## Règle de gestion des données dans le référentiel

Une donnée doit se trouver dans le référentiel :

* **SI** elle est présente dans au moins 2 applications consommatrices en aval

**OU**

* **SI** elle est présente dans une application qui alimente le référentiel en amont ET dans une application consommatrice en aval

## Les données

Afin de ne pas se perdre, nous avons dans un premier temps limité le nombre de données considérées comme essentielles et d’autant plus susceptibles d’être re-saisies et stratégiques.

## Les métadonnées

## Dotations et services fournis par catégorie de population

Pour chaque population, les écoles ont défini un package de services avec des éventuelles limitations. Nous parlons principalement de services numériques mais pas exclusivement (ex : fourniture d’un badge).

Dotations en matériels

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Population / Services** | Badge Contrôle d’accès **(1)** | Compte **(2)** | Email **(3)** | WIFI **(4)** | Impression **(5)** | ENT **(6)** | Restaurant | Bibliothèque |
| Etudiants |  |  |  |  |  |  |  |  |
| Permanents en CDI |  |  |  |  |  |  |  |  |
| Personnels en CDD |  |  |  |  |  |  |  |  |
| Vacataires |  |  |  |  |  |  |  |  |
| Apprentis |  |  |  |  |  |  |  |  |
| Stagiaires |  |  |  |  |  |  |  |  |
| Doctorants contrat doctoral |  |  |  |  |  |  |  |  |
| Doctorants non payés |  |  |  |  |  |  |  |  |
| Post-Doc |  |  |  |  |  |  |  |  |
| Sabbatiques et Chercheurs invités |  |  |  |  |  |  |  |  |
| Personnels CNRS |  |  |  |  |  |  |  |  |
| Personnels associés ou invités |  |  |  |  |  |  |  |  |
| Professeurs émérites ou Maîtres de Conférence Honoraires |  |  |  |  |  |  |  |  |
| Incubés |  |  |  |  |  |  |  |  |
| Retraités |  |  |  |  |  |  |  |  |
| Extérieurs |  |  |  |  |  |  |  |  |
| Associations, clubs |  |  |  |  |  |  |  |  |
| Syndicats |  |  |  |  |  |  |  |  |
| Comptes systèmes |  |  |  |  |  |  |  |  |

Badges **(1)**

Adresses mail personnelles **(3)**

WIFI **(4)**

Impressions et quotas associés **(5)**

Bibliothèque

Cas particulier des professeurs émérites

## Applications sources

**Les applications sources sont celles qui vont détenir l’information d’origine et alimenter le référentiel.** En reprenant pour chaque population, le tableau des données du chapitre 3.2, on peut lister le nom de l’application source.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ETUDIANTS | PERSONNEL | VACATAIRES | DOCTORANTS | EXTERIEURS |
| Nom |  |  |  |  |  |
| Prénom |  |  |  |  |  |
| Email |  |  |  |  |  |
| Rattachement |  |  |  |  |  |
| Date naissance |  |  |  |  |  |
| Date arrivée |  |  |  |  |  |
| Date départ |  |  |  |  |  |
| Photo |  |  |  |  |  |
| Identifiant |  |  |  |  |  |
| Identifiant unique |  |  |  |  |  |

## Applications consommatrices

Les applications consommatrices sont celles qui vont **consommer l’information dans le référentiel**. Il est important de les lister car cela va permettre de déterminer si l’information traitée doit être stockée ou pas dans le référentiel. *Si une donnée est présente dans une application d’origine mais n’est jamais réutilisée dans aucune autre application, il est inutile de la stocker dans le référentiel.*

Pour constituer un tableau par population, on s’inspire complètement du travail d’analyse réalisé au sous-chapitre précédent.

Population = Etudiant

Population = Personnel

Population = Vacataire

Population = Acteur recherche

Population = Extérieur

Ce tableau permet également d’identifier le nombre de ré-saisies manuelles actuelles et d’en diminuer le nombre.

## Le référentiel des organisations

Le référentiel des organisations ou encore le référentiel des structures organisationnelles joue un rôle essentiel. Il permet de refléter l’organisation et de faire des liens avec les personnes.

Ces liens vont permettre l’obtention de rôles d’où découleront des autorisations pour l’accès aux services utilisateurs.

On peut imaginer qu’à partir de ce référentiel des organisations on soit capable de reconstruire un organigramme de façon automatique.

## Les groupes

Cette fonction vise à centraliser la gestion des groupes utilisateurs.

Elle permet d’attribuer des rôles parfois indépendants des structures organisationnelles avec une vision plus fonctionnelle. L’appartenance à un groupe permettra d’y associer l’ouverture à un service.

Voici, dans un premier temps, la liste de ces services.

# La vision cartographie et process

Dans ce chapitre, nous adoptons une vision process en partant de la cartographie applicative actuelle. Pour chaque population et chaque application, nous analysons les données qui transitent, les applications sources pour alimenter le référentiel et celles qui vont consommer ces données.

On peut ainsi constituer une référence des données transitant entre les applications du SI ce qui va consolider notre vision du référentiel des personnes.

Le code couleur suivant a été adopté pour distinguer les données lues, écrites ainsi que les filtres.

* Vert : lecture
* Rouge : écriture
* Bleu : filtres

## Création des comptes

Propriétaire du process :

## Authentification AD

Propriétaire du process :

## Transmission des informations vers le restaurant

Propriétaire du process :

## Génération du code lecteur Médiathèque

Propriétaire du process :

## Récupération des adresses mails étudiants

Propriétaire du process :

## Edition des badges et cartes étudiants

Propriétaire du process :

## Mise à jour et affichage de l’annuaire page blanche

Propriétaire du process :

## CVtheque

Propriétaire du process :

## Synchronisation avec le LMS Moodle

Propriétaire du process :

## Synchronisation avec Zimbra

Propriétaire du process :

## Récupération des mobilités de stage

Propriétaire du process :

## Affectation des droits dans l’ENT esup-portail

Propriétaire du process :

## Changement du mot de passe

Propriétaire du process :

## Droits d’accès à certaines ressources en salle de T.P.

Propriétaires du process :

## Accès au Helpdesk GLPI

Propriétaires du process :

# Architecture TECHNIQUE cible

Ce chapitre a pour objectif de définir une architecture technique cible pour héberger le référentiel des personnes, les données et les interfaces à mettre en place avec les différentes briques du système d’information.

Ce chapitre doit donc répondre à un certain nombre de questions parmi lesquelles.

# ASPECTS JuridiqueS : CNIL & DPO

Ce chapitre traite des aspects juridiques qui ne doivent surtout pas être négligées.

Le premier travail va consister à mettre à jour les registres en fonction des évolutions suite au départ de notre CIL.

Le deuxième travail va consister à nommer un correspondant au DPO

En effet, l’application en France de la Directive européenne RGPD (Régime Général de Protection de Données) le 25 mai 2018 va avoir un impact important sur le traitement des données personnelles et donc sur les applications et les process.

A partir de cette date, les utilisateurs devront être informés de l’usage de leurs données et en principe donner leur accord pour le traitement de leurs données, ou pouvoir s’y opposer : il s’agit de **l’expression du consentement**. La charge de la preuve du consentement incombe au responsable de traitement.

**Le droit à la portabilité** quant à lui doit offrir aux personnes la possibilité d’accéder à ses données personnelles et à les récupérer.

Cela pose plusieurs questions.

Faut-il continuer à publier les informations des personnes par défaut sur Internet ?

De la même façon, il faut offrir une façon simple à l’utilisateur d’accéder aux données personnelles qui le concernent. C’est ce qu’offre le logiciel **Fusion Directory**.

Il faut sans doute multiplier les accords de communication de ces informations à des entités juridiques différentes avec lesquelles les écoles du campus travaillent : l’association des Alumni pour les anciens, etc …

Enfin, il faut renforcer et décrire les mécanismes pour sécuriser l’accès à ces données.

# ANNEXE 1 : DETAILS DE LA METHODOLOGIE

Pour identifier les données qui doivent être gérées dans le référentiel, l’équipe a défini une méthodologie qui a été appliquée dans ce document.

Définition d’une règle pour l’insertion dans le référentiel

Listing des principales données

L’équipe a commencé par lister les principales données manipulées par les applications. Afin de simplifier l’analyse, nous avons, dans un premier temps, restreint le nombre de données à une dizaine.

Exemple 1 :

|  |
| --- |
| Population = Etudiant |
| Nom |
| Prénom |
| Date naissance |
| Photo |
| Entité rattachement |
| Date d’arrivée |
| Date de départ |
| Identifiant unique |
| … |

SI Formation

Définition des services fournis par population

Dans un deuxième temps, on définit pour chaque catégorie de population, les services qui seront délivrés.

Exemple 2 :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Population** | Badge | Compte | Email | WIFI | …/… | ENT | MinTel Congés |
| Etudiants | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non |
| Permanents en CDI | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non |

Identification des applications sources

Un troisième tableau liste l’ensemble de ces données en identifiant l’application source ou génératrice associée.

Exemple 3 :

|  |  |
| --- | --- |
| Population Etudiant | Concours |
| Nom | Concours |
| Prénom | Concours |
| Identifiant unique | SI Formation |
| Entité de rattachement | Concours |
| Date d’arrivée | SI Formation |
| Date de départ | SI Formation |
| Photo | Inscription en ligne |
|  |  |
|  |  |

Tableau des applications consommatrices

Le passage en revue de toutes les applications, réalisé à l’étape précédente va permettre de lister, pour chaque donnée, l’ensemble des applications utilisatrice de cette même donnée.

On constitue donc un tableau final de ce type.

|  |  |  |
| --- | --- | --- |
| Donnée | Application source | Applications consommatrices |
| Population = étudiant | Concours | SI formation, ecampus, Moodle… |
| Nom | Concours |  |
| Prénom | Concours |  |
| Identifiant unique | SI Formation |  |
| Entité de rattachement | Concours |  |
| Date d’arrivée | SI Formation |  |
| Date de départ | SI Formation |  |
| Photo | Inscription en ligne | … |
|  |  |  |
|  |  |  |

Approche process

Afin de compléter cette vision, l’équipe est repartie de la cartographie applicative et, à partir de chaque application référencée et pour chaque population, a indiqué si elle était simplement consommatrice de cette donnée ou si c’était l’application source générant la donnée (en rouge).

On arrive ainsi à constituer une cartographie des flux de données entre les applications afin d’éviter les ré-saisies et fiabiliser les données.

# ANNEXE 2 : Définition des POPULATIONS

Cette annexe définit succinctement les différentes catégories de populations gérées dans le référentiel des personnes.

Etudiants

Permanents en CDI

Personnels en CDD

Vacataires

Apprentis

Stagiaires

Doctorants contrat doctoral

Doctorants non payés

Post-Doctorants

Sabbatiques et Chercheurs invités

Personnels CNRS

Personnels associés ou personnels invités

Professeurs émérites ou Maîtres de Conférence Honoraires

Retraités

Extérieurs

Association /club

Syndicat

Système

# ANNEXE 3 : Referentiels d’Organisation

Voici l’organisation au (date) de (entité client).

[Olivier EPINETTE](https://trombi.imtbs-tsp.eu/index.php?user=Olivier EPINETTE&dpt=PEM&sub=n)

* + [Direction du Développement et de la Valorisation](javascript:affArbo('INTM_DDVEM'))

[Fabrice BERNARD](https://trombi.imtbs-tsp.eu/index.php?user=Fabrice BERNARD&dpt=SS&sub=n)

# ANNEXE 4 : CARTOGRAPHIE APPLICATIVE

Cartographie applicative en date du

# ANNEXE 5 : Schéma OpEnLdap