

3iL Rodez 2017

**Rapport de projet web**

**Bourse aux livres**

**Kristen VIGUIER & Simon BAUMANN**

Sommaire

[Conception 2](#_Toc482656325)

[Définition du besoin 2](#_Toc482656326)

[Règles de gestion 2](#_Toc482656327)

[Fonctionnalités métiers 4](#_Toc482656328)

[Règles organisationnelles 5](#_Toc482656329)

[Diagramme de classe 7](#_Toc482656330)

[MCD / MLD 7](#_Toc482656331)

[Diagramme de flux 7](#_Toc482656332)

[Diagrammes de cas d’utilisation 7](#_Toc482656333)

[Synthèse de gestion de projet 8](#_Toc482656334)

[Méthodologie utilisée 8](#_Toc482656335)

[Outils de gestion de projet 8](#_Toc482656336)

[Fonctionnalités implémentés / non-implémentés 9](#_Toc482656337)

[Fonctionnalités implémentés par page 9](#_Toc482656338)

[Fonctionnalités non-implémentés : 10](#_Toc482656339)

[Bonnes pratiques mises en œuvre 11](#_Toc482656340)

[Installation du site 12](#_Toc482656341)

[Fonctionnement du code 12](#_Toc482656342)

# Conception

## Définition du besoin

Mise en place d’un système informatique pour l’association APERO (Association des Parents d’Elèves de Rodez-Onet) permettant aux familles d’assurer le dépôt et la vente de manuels scolaire de l’année écoulée.

## Règles de gestion

**Décote des manuels repris :**

|  |  |  |
| --- | --- | --- |
|  | Décote | Durée utilisation en général |
| Très bon état | 25 % | 1 an |
| Bon état | 40 % | 2 ans |
| Assez bon état | 50 % | 3 ans |
| Endommagé | 65 % | Plus de 3 ans |

**Le calcul des paiements :**

Ce calcul doit être automatiquement pris en charge par le système informatique.

Nous avons connaissance des manuels vendus par famille ainsi que le prix de vente du manuel.

Il y a deux cas :

* Le montant de la vente des livres est inférieur à 100 euros :

On retient 20% sur le montant de la vente et la cotisation est offerte

**Total à payer** = **sommePrixManuelsVendus** x **0.8**

* Le montant de la vente est supérieur à 100 euros :

On retient 10% sur le montant de la vente et on retire 10 euros de cotisation

**Total à payer** = **(sommePrixManuelsVendus** x **0.9) - 10**

**Règles liées la secrétaire :**

La secrétaire appelle les établissements pour obtenir la liste des ouvrages (par classe et section).

La secrétaire cherche le prix des ouvrages neufs et les saisies dans le système informatique pour que les bénévoles puissent établir ultérieurement les prix des manuels d’occasions.

**Règles liées aux dépôts :**

Le dépôt des manuels se fait par les familles adhérentes dans les locaux de l’association. Un bénévole réceptionne et expertise les manuels des familles.

Seul les manuels en usage pour l’année suivante seront repris si réutilisables (états + usage pour année N+1).

Pour qu’une famille puisse déposer un manuel, il faut qu’elle soit déjà adhérente ou qu’elle adhère à l’association. Pour cela elle paye une cotisation qui sera retenue sur la vente des manuels.

La famille ayant adhéré peut ensuite déposer autant de manuels qu’elle souhaite si les manuels remplissent les conditions de reprise.

**Règles liées à la vente :**

Un bénévole vend des manuels aux acheteurs qui sont obligatoirement des familles adhérentes, durant la période de mi-juillet à fin juillet et de fin août à mi-septembre.

La semaine suivant la rentrée des classes, la vente de manuels devient libre (aux familles non adhérentes).

Un acheteur paye les manuels qu’il souhaite exclusivement par chèque au nom de l’association.

**Règles liées à la cotisation :**

La cotisation des familles qui souhaitent déposer des manuels s’élève à 10 euros.

La cotisation des familles adhérentes lors de la vente (qui n’ont pas déposé) est de 5 euros.

**Règles liées au retrait de manuels :**

Une fois les périodes de vente de manuels terminées, les adhérents peuvent venir récupérer les manuels invendus auprès de la secrétaire.

Si certains manuels n’ont pas été retirés, alors la secrétaire remettra les manuels non retirés à des associations caritatives.

## Fonctionnalités métiers

**Détail des fonctionnalités métiers de la secrétaire :**

Période fin mai à début-juin

* Liste des établissements scolaires
* Enregistrer la liste officielle des ouvrages
* Saisir du prix des ouvrages neufs

Période fin septembre

* Calcul des paiements à effectuer et impression d’une lettre chèque automatique
* Lister les vendeurs pour obtenir information car doit envoyer lettre chèque

Période tout le mois d’octobre

* Retrait des manuels invendus (lister les manuels non vendus)

**Détail des fonctionnalités métiers des bénévoles :**

Période mi-juin à mi-juillet (dépôt des manuels)

* Inscription des adhérents de l’association (payer 10 € retenu sur la vente)
* Réception et expertise des manuels
* Attribution d’une décote (seulement manuel en usage l’année prochaine)
* Enregistrement des manuels réceptionnés en BDD (numéro étiquette adhésive, calcul de son prix à partir des ouvrages neuf en appliquant la décote)
* Fiche récapitulative doit être fourni (imprimé pour le déposant)

Période de mi-juillet à fin-juillet de fin-août à mi-septembre

* Vente des livres (Bénévole s’assure qu’il s’agit bien d’un adhérent, paiement par chèque)
* Réserver aux adhérents (doivent payer 5€)
* Si stock non épuisé avant rentré des classes alors vente ouverte aux non adhérents.
* Inscription de l’acheteur en bdd
* Etablissement d’une facture avec remise des manuels

## Règles organisationnelles

**Vente de manuels :**

Trois équipes de deux personnes les premières journées des deux périodes de vente.

Liste de livres

Equipe

Acheteur

Vérifie ou Enregistre les coordonnées de l’acheteur

Proposer à l’acquéreur

Accord

Arrêt procédure achat

Facture + remise manuel

Chèque incluant éventuellement la cotisation

1ère Pers

2ème Pers

Recherche manuels disponibles

Manuel disponible

Refus

**Dépôt de manuels :**

*Deux équipes de bénévoles :*



1 ordinateur

1 ordinateur

2 personnes

2 personnes

*Fonctionnement de l’équipe :*



Personne 2

Numérote avec étiquette

Attribue décote

Examine manuels remis

Accueille

Personne 1

Enregistre les données (au fur et à mesure)

Vérifie état (rejet éventuel)

Impression et remise d’une fiche récapitulative au déposant

Chaque soir, les manuels déposés sont stockés dans des bacs. La journée suivante, ils seront mis en rayonnage.

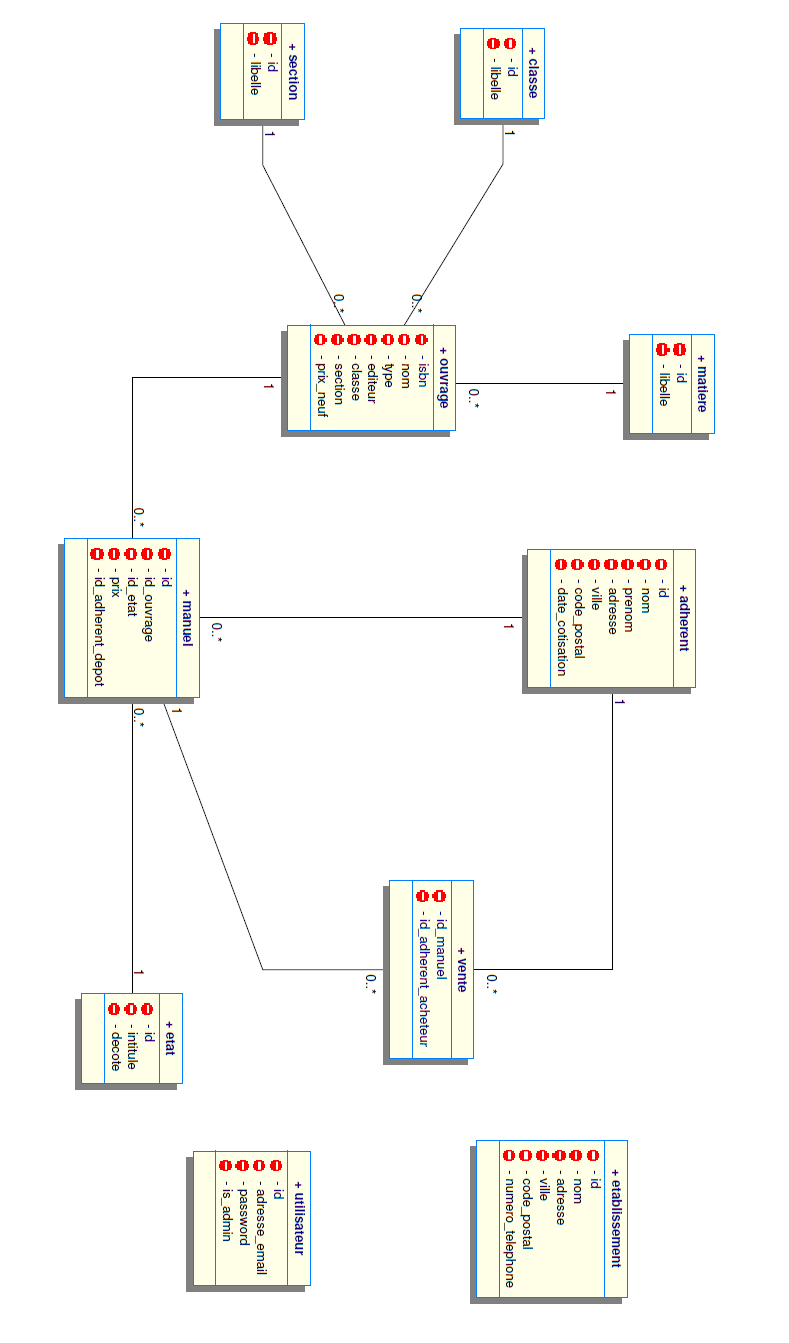
**Paiement des familles adhérentes :**

Le calcul de paiement à effectuer auprès des familles se fait automatiquement par le site web, en fonction des livres vendus. L’impression d’un récapitulatif se fait par les bénévoles via le site.

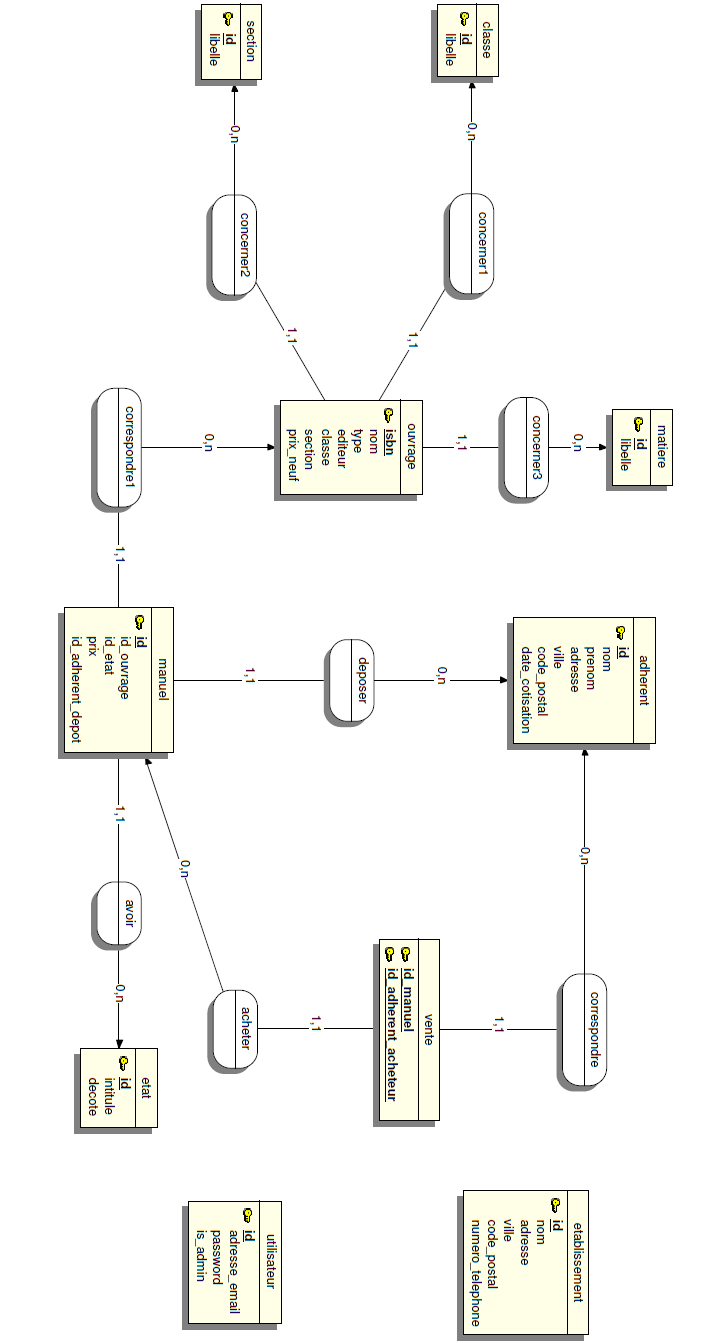
## Dictionnaire des données

|  |  |  |  |
| --- | --- | --- | --- |
| Attribut | Description | Type | Valeur |
| id | Identifiant unique de l’adhérent | INT | 2 |
| nom | Nom de famille de l’adhérent | TEXT | Dupont |
| prenom | Prénom de l’adhérent | TEXT | Bob |
| adresse | Adresse de l’adhérent | TEXT | 6 rue des coquelicots |
| ville | Ville de l’adhérent | TEXT | Rodez |
| code\_postal | Code postal de l’adhérent | TEXT | 12000 |
| date\_cotistation | Date à laquelle l’adhérent à cotisé ou null | DATE | 10/10/2010 |
|  |  |  |  |
| id | Identifiant unique de l’ouvrage | INT | 1 |
| nom | Nom de l’ouvrage | TEXT | Exos&Méthodes |
| editeur | L’éditeur de l’ouvrage | TEXT | Nathan technique |
| Type | Type de l’ouvrage (mathématiques, français…) | TEXT | Mathématique |
| classe | La classe auquel correspond l’ouvrage | TEXT | 1ere |
| section | La section auquel correspond l’ouvrage | TEXT | S |
| prix\_neuf | Prix de l’ouvrage neuf | NUMBER | 7,00 |
|  |  |  |  |
| isbn | code isbn unique du manuel | INT | 1 |
| id\_ouvrage | Identifiant permettant de rattacher le manuel à un ouvrage | INT | 1 |
| id\_etat | Identifiant permettant de définir un état au manuel | INT | 2 |
| prix | Prix du manuel avec décote | TEXT | 4,00 |
| id\_adherent\_depot | Identifiant de l’adhérent qui a déposé ce manuel | INT | 12 |
|  |  |  |  |
| id | Identifiant de la matière | INT | 1 |
| libelle | dénomination de la matière liée à un ouvrage | TEXT | mathématiques |
|  |  |  |  |
| id | Identifiant unique de l’établissement | INT | 5 |
| nom | Nom de l’établissement | TEXT | Lycée François d'Estaing |
| adresse | Adresse de l’établissement | TEXT | 22 Boulevard Denys Puech |
| code\_postal | Code postal de l’établissement | TEXT | 12000 |
| ville | Ville de l’établissement | TEXT | Rodez |
| numero\_telephone | Numéro de téléphone de l’établissement | TEXT | 05 65 77 17 00 |
|  |  |  |  |
| id | Identifiant unique de la classe | INT | 1 |
| libelle | Libelle-nom de la classe | TEXT | Première |
|  |  |  |  |
| id | Identifiant unique de la section | INT | 1 |
| libelle | Libelle-nom de la section | TEXT | ES |
|  |  |  |  |
| id | Identifiant unique de l’état | INT | 2 |
| intitule | Intitulé de l’état | TEXT | Bon état |
| decote | Décote (pourcent) en fonction de l’état | INT | 25 |
|  |  |  |  |
| id\_manuel | Identifiant unique du manuel vendu | INT | 1 |
| id\_adherent\_achat | Identifiant unique de l’adhérent acheteur | INT | 1 |
|  |  |  |  |
| id | Identifiant unique d’un utilisateur du site | INT | 1 |
| adresse\_email | login de connexion au site | TEXT | benev@xxx.com |
| mdp | mot de passe de connexion au site | TEXT | motdepasse |
| is\_admin | l’utilisateur est Admin ou non | BOOLEAN | TRUE |

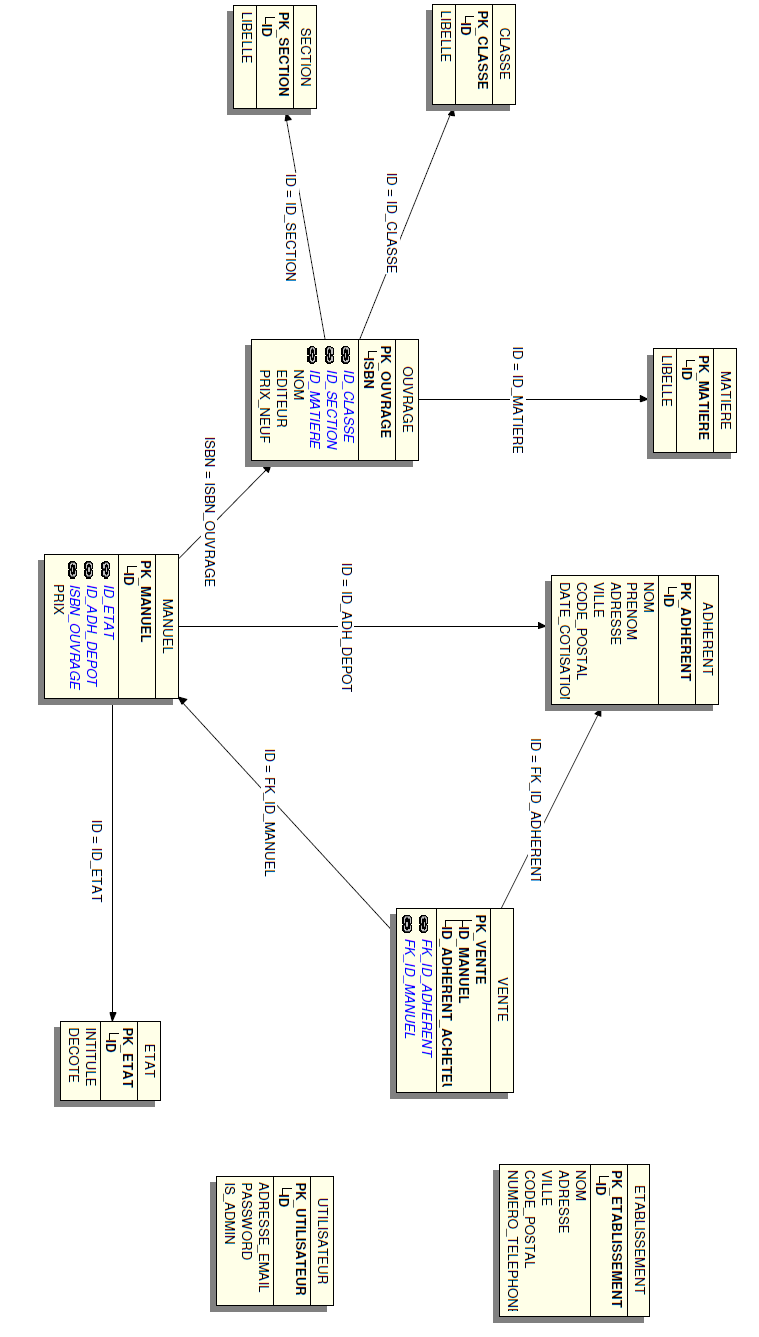
## Diagramme de classes



## MCD



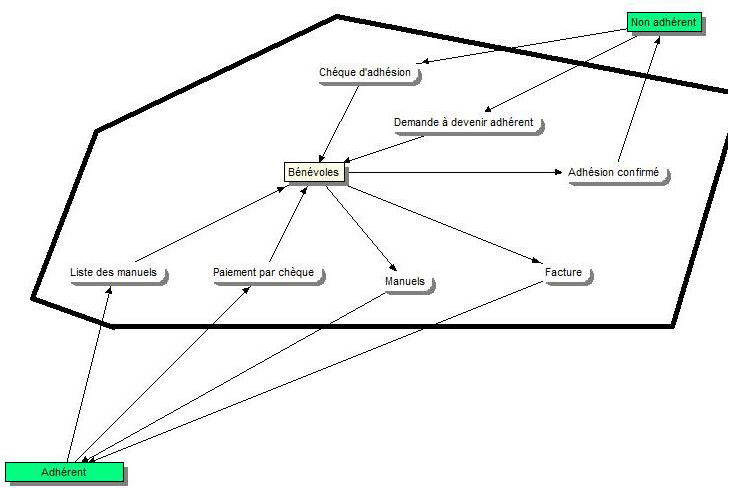
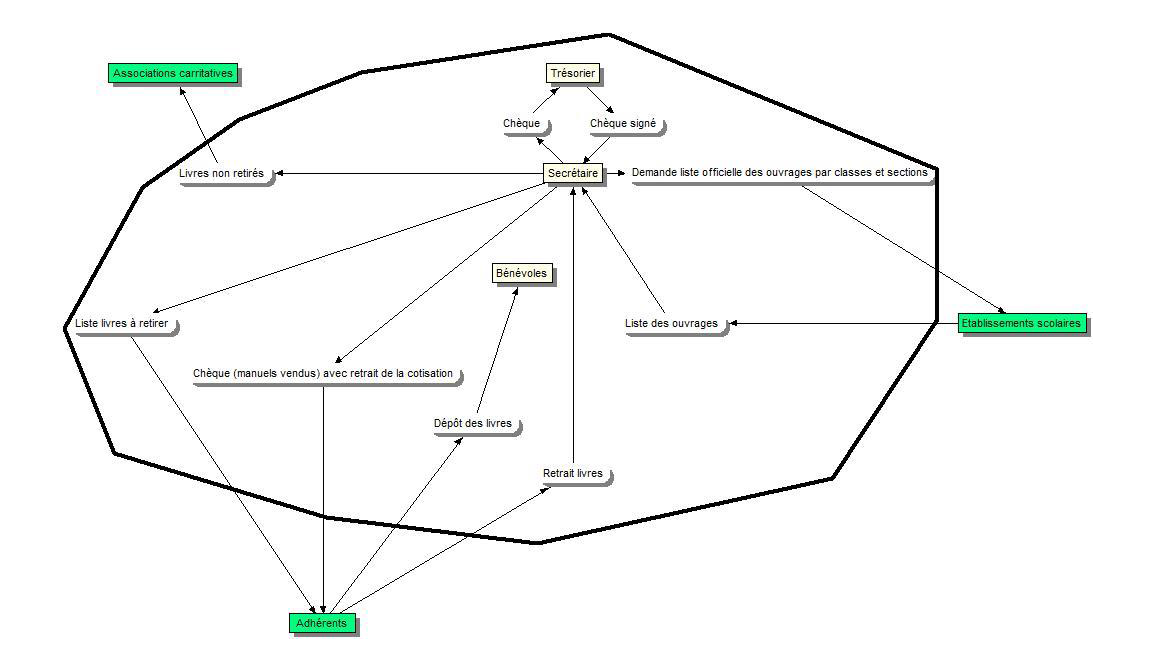
## MLD



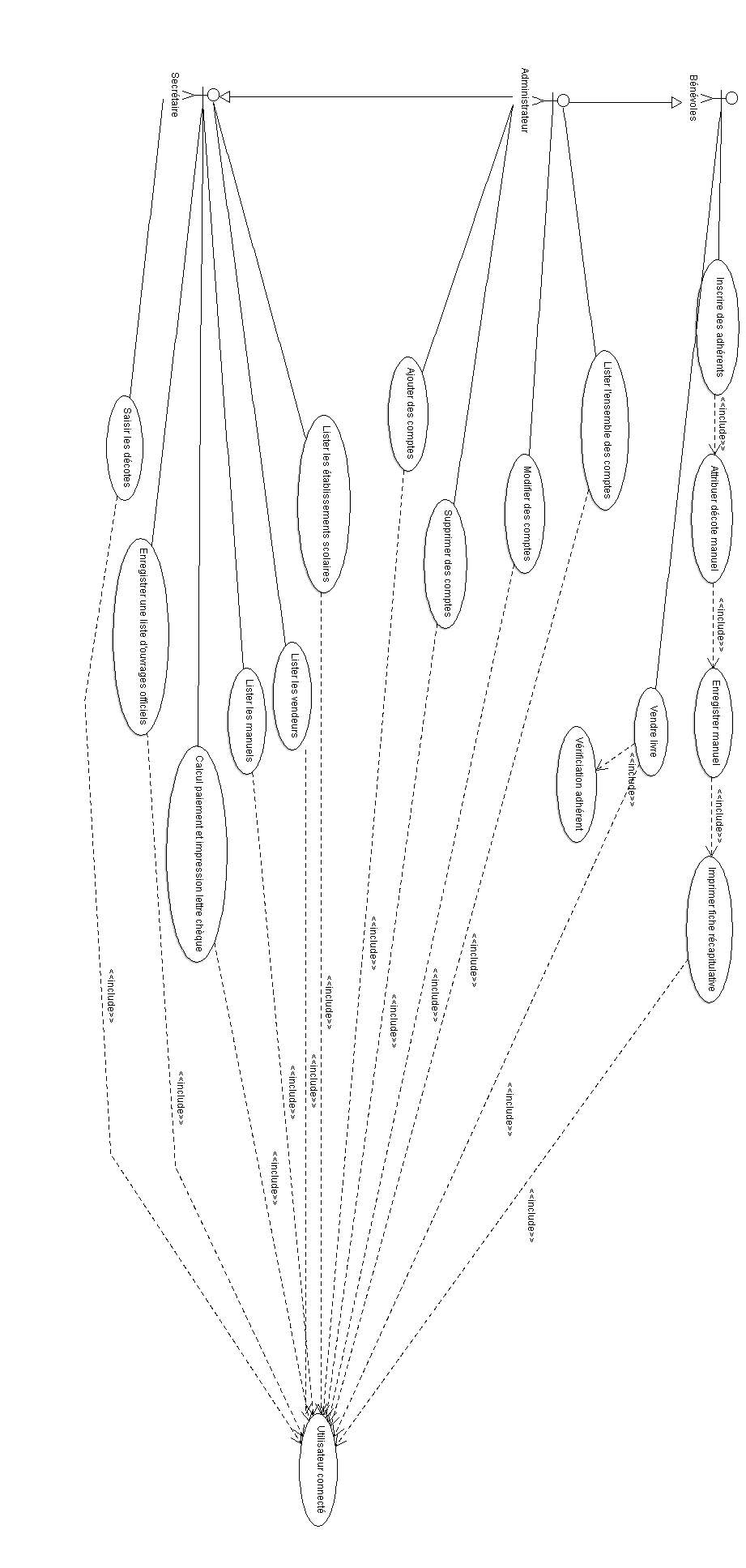
## Diagramme de flux

### Période hors vente

### Période de vente



## Diagrammes de cas d’utilisation



# Synthèse de gestion de projet

## Méthodologie utilisée

Pour réaliser ce projet informatique, nous avons choisi d’utiliser une méthode de gestion de projet similaire à celle du **Cycle en V** pour les raisons suivantes :

* Les spécifications des besoins utilisateurs sont établies au préalable par le client. Toutes les informations utiles à la conception de l’application sont exprimées dans le cahier des charges. Nous avons cependant demandé quelques précisions au client qui a su nous exprimer clairement ses attentes.
* Nous avons réalisé la conception architecturale de l’application ainsi que la conception détaillée en amont, juste après avoir analysé en profondeur le cahier des charges. Un diagramme de Gantt a été réalisé pour avoir un aperçu des tâches à réaliser dans le temps qui nous était imparti. Le MCD/MLD/Diagramme de classe/Diagramme de flux ont ensuite été produit pour anticiper les besoins lié au codage de l’application web.
* La fin de la conception globale a donné suite à la création de la base de données sur phpMyAdmin.
* Phase de codage et développement : …………………………………………………. ?
* Les tests réalisés ont étés réalisés directement par le biais de l’interface IHM de l’application. Les tests unitaires et les tests d’intégrations n’ont pas été menés dû à une contrainte de temps qui nous a été imposé.
* Parallèlement au développement de l’application, nous avons rédigé ce rapport afin qu’il soit le plus complet possible.

## Outils de gestion de projet

Afin de pouvoir suivre en permanence l’avancement du projet et de mettre en commun les travaux réalisés, nous avons choisis d’utiliser le logiciel de gestion de version décentralisé Git. Par ailleurs, nous avons lié notre répertoire git local à la plateforme GitHub pour visualiser notre projet dans un environnement cloud.

Pour réaliser le diagramme de Gantt relatif à notre projet, nous avons utilisé le logiciel ????

Diagramme de Gantt avec la répartition des tâches

Screenshot projet GitHub

# Fonctionnalités implémentés / non-implémentés

## Fonctionnalités implémentés par page

**Connexion**

La page de connexion est le point d’entrée du site.  
Un utilisateur ne peut exploiter le site sans s’être authentifié en tant qu’administrateur ou simple utilisateur (bénévole ou secrétaire).

**Utilisateurs**

* Des comptes utilisateur ont étés implémentés afin de permettre à la secrétaire et aux bénévoles de se connecter au site web
* Pour simplifier l’application, nous avons regroupé les fonctionnalités utilisés par la secrétaire et les bénévoles en un seul type de compte
* Il est possible de modifier le mot de passe de son compte, lorsque l’on est connecté

**Ouvrages**

* Ajouter un nouvel ouvrage à la base de données
* Lister les ouvrages en récupérant les informations à afficher dans la base de données
* Supprimer un ouvrage de la base de données

**Adhérents**

* Ajouter un nouvel adhérent
* Lister les adhérents et leurs informations présents dans la base de données
* Supprimer un adhérent de la base de données

**Administrateur**

* Ajouter un nouvel utilisateur pouvant se connecter au site (non-admin ou admin)
* Lister les utilisateurs présents en base de données
* Ajouter ou retirer les droits administrateurs d’un compte
* Supprimer un utilisateur de la base de données

**Dépôt**

**Vente**

## Fonctionnalités non-implémentés :

* Permettre la création de comptes disposant de fonctionnalités utilisables uniquement par la secrétaire et pareil pour les bénévoles. Cela éviterai que des mauvaises manipulations puissent se produire.
* Afficher un indicateur dans la page des adhérents afin que les bénévoles puissent savoir si une famille a déjà payé la cotisation.
* Pouvoir afficher la liste de tous les manuels invendus.
* Le système de dépôt de livres fonctionnel
* Le système de vente de livres fonctionnel (avec récapitulatif)

A compléter

# Bonnes pratiques mises en œuvre

**Les commentaires**

Des commentaires clairs et explicites ont été écrits au fur et à mesure du développement pour que notre application soit la plus maintenable possible, qu’il n’y ait pas d’ambiguïté. Sachant qu’il a une différence de niveau en programmation web dans le groupe, les commentaires ont été fondamentaux pour que l’on puisse tous les deux comprendre le code et continuer le développement de chacun.

**La documentation**

Nous fournissons une documentation (manuel utilisateur) pour les utilisateurs du site web, dans laquelle sont détaillées toutes les fonctionnalités disponibles.

**La gestion des erreurs**

Une gestion d’erreurs poussée a été mise en place, tout au long du développement du site web.

**La gestion de la sécurité**

Plusieurs failles fondamentales sont gérées :

* Failles XSS (Cross-Site Scripting) est une faille permettant l’injection de code HTML ou javascript. Nous avons réalisé un contrôle de saisie en appliquant le « Never Trust User Input ». Nous avons déspécialisé et appliqué des contrôles sur toutes les saisies venant de l’utilisateur avant de réaliser des actions ou requête à la BDD.
* La faille include est dû à une mauvaise utilisation de la fonction include(). Il faut tester l’existence du fichier à include avant de réaliser l’action et mettre en place un fichier htaccess.
* L’injection SQL qui consiste à modifier une requête SQL en injectant des morceaux de code non filtrés soit par le biais d’un formulaire ou alors par le biais de l’URL en modifiant les paramètres. Filtrage de données récupérées par URL + déspécialisation des données + utilisation des requêtes préparées avec PDO.
* La faille CSRF n’a pas été mise totalement en pace, le token est présent mais le contrôle des formulaires n’a pas pu être implémenté par manque de temps. Cette faille consiste à faire réaliser des actions à l’utilisateur à son insu.
* Attaque par force brute non implémentée par manque de temps. Solution pour future évolution mettre en place un captcha sur la saisie des formulaires.

**La réutilisation**

Je te laisse compléter

**L’anticipation des évolutions**

# Installation du site

Si vous souhaitez installer votre site chez vous en local ou tout simplement le déployer chez un hébergeur, il vous faudra réaliser quelques paramétrages pour que le site soit fonctionnel.

Il vous faudra vous rendre dans le dossier config. Vous trouverez 5 fichiers php, seulement deux sont à modifier : il vous faudra dans un premier temps éditer le fichier « const.php » à adapter, vous y trouverez une section /\* BASE DE DONNÉES \*/ qui contient les logs de connexion, l’adresse IP du serveur SQL ainsi que le nom de la base de données. Vous trouverez aussi une balise /\* PARAMETRES \*/, si vous passez en mode développement ou production une constante « AFFICHER\_ERREURS » doit être modifiée en vrai ou faux. Dans la section /\* PATH \*/ il vous faudra penser à changer l’adresse absolue de votre site dans la constante « ADRESSE\_ABSOLUE\_URL ».

Avant d’ouvrir la page « index.php », la base de données doit être créée et le nom doit correspondre avec celui du fichier « const.php » dans la section /\* BASE DE DONNÉES \*/. Vous pouvez prendre le fichier SQL afin de le modifier à votre guise pour avoir des données personnalisées.

# Fonctionnement du code

Afin de faciliter la compréhension du code et, par conséquent, sa maintenance, il est nécessaire d’expliquer son fonctionnement.

Nous avons utilisé une architecture 3-tiers MVC (Modèle Vue Contrôleur) : le modèle permet de réaliser des interactions entre le site et la base de données, le contrôleur réalise des traitements sur les données remontées par le modèle afin d’en faire profiter la vue qui structure la page web. Dans le dossier du site « bourseauxlivres », il existe trois dossiers nommés « modele », « vue » et « controleur » correspondant à ces trois couches. En cas de modification de la structure d’une page, il faudra donc aller dans le dossier « vue ».

Le point d’entrée du site est toujours le fichier « index.php », tous les chargements de pages se font par lui. Il inclut les fichiers de configuration du site (l’accès à la base de données, les constantes, un tableau des pages existantes, un fichier de configuration pour le chargement de fichier et un fichier de code retour).

On peut décider d’afficher les erreurs ou non (c’est utile pour le développement), il faudra donc penser à définir la constante AFFICHER\_ERREURS à false lors de la livraison du projet. On vérifie l’existence de paramètre dans l’url, on se protège d’éventuelles injections en parcourant chacune des variables globales en déspécialisant les caractères spéciaux.

Le nom de la page est toujours passé par URL, on vérifie donc si elle existe bien dans notre tableau de pages existantes. Si c’est le cas alors nous incluons le contrôleur et la vue associés sinon une page d’erreur. Explication plus détaillée sur l’url : nous avons fait de la réécriture d’url ce qui a l’avantage d’être plus lisible pour l’utilisateur, de masquer certaines données. Nous récupérons donc ces paramètres par un GET, on explose la chaîne en segment : le premier élément correspond toujours à la page tandis que le reste correspond à des paramètres passés par URL.