UNIVERSITÉ DU BURUNDI
GRENIER DU SAVOIR DU BURUNDI
Dépôt institutionnel officiel
https://repository.ub.edu.bi

Mise en place d’une application informatiquesécurisée pour la gestion du systèmepénitentiaire de la République Démocratique duCongo

BORIBO KIKUNDA, Philippe

2020-01
UB
https://repository.ub.edu.bi/handle/123456789/246

Document téléchargé depuis le **Grenier du Savoir du Burundi** — https://repository.ub.edu.bi

République du Burundi
Ministère de l'Éducation Nationale et de la Recherche Scientifique

Université du Burundi
Faculté des Sciences de l'Ingénieur



Département de TIC

Master en Génie Informatique
Année académique : 2019-2020

MEMOIRE

Présenté à la

Faculté des Sciences de l'Ingénieur (FSI)

En vue de l'obtention du diplôme de

MASTER

en

Génie Informatique

Par

BORIBO KIKUNDA Philippe

Mise en place d'une application informatique sécurisée pour la gestion du système pénitentiaire de la République Démocratique du Congo

Soutenu le 07/05/2021, devant le jury composé de :

Pr	NDIKUMAGENGE Jérémie	Président
Dr	SAHINGUVU William	Vice-Président
Pr	MANIRABONA Audace	Sécrétaire
Dr	NDAYISABA Longin	Directeur
Dr	MUKESHIMANA Michèle	Membre

IDENTIFICATION DES MEMBRES DU JURY

Dr	NDAYISABA Longin	: Directeur de thèse
Pr	NDIKUMAGENGE Jérémie	: Président du jury
Dr	SAHINGUVU William	: Vice-Président
Pr	MANIRABONA Audace	: Secrétaire
Dr	MUKESHIMANA Michèle	: Membre

DÉDICACES

A ma femme et mes enfants, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chers parents Ildéphonse et Jeanine pour leurs encouragements permanents, et leur soutien moral,

A mes chers frères et sœurs, David, Musa, Magy, Nyota pour leur appui et leur encouragement,

A toute ma famille pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infaillible,

Merci d'être toujours là pour moi.

BORIBO KIKUNDA Philippe

REMERCIEMENTS

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.

Je tiens à exprimer tout d'abord toute ma reconnaissance à mon directeur de mémoire, Monsieur Dr. NDAYISABA Longin. Je le remercie de m'avoir encadré, orienté, aidé, conseillé et surtout donné goût à sécuriser mes données.

J'adresse mes sincères remerciements à tous les professeurs, intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions et ont accepté de me rencontrer et de répondre à mes questions durant mes recherches.

Je remercie ma tendre épouse Grace, ainsi que mes deux enfants Gaël et Jess qui ont toujours été là pour moi. Je remercie mes parents Ildéphonse et Jeanine, et mon frère David, pour leurs encouragements.

Enfin, je remercie mes amis et collègues de promotion Vincent, Alain, Hussein, Musseven, Tshibangu, Ruffin... qui ont toujours été là pour moi. Leur soutien inconditionnel et leurs encouragements ont été d'une grande aide.

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

SIGLES ET ABRÉVIATIONS

COCOMO	COnstructive COst Model
CPC	Code de Procédure civile
CPP	Code de Procédure Pénale
CRUD	Create Read Update Delete
CSS	Cascading Style Sheets
HM	Homme-Mois
HTML	HyperText Markup Language
MAA	Maison d'arrêt Annexe
MONUSCO	Mission des Nations Unies au Congo
MVC	Modèle-vue-contrôleur
NF	Non Fonctionnel
NTIC	Nouvelles Technologies de l'Information et de la Communication
OAEP	Optimal Asymetric Encryption Padding
PC	Prison centrale
PDD	Prison de District
PDP	Prison de Police
PHP	Hypertext Preprocessor
PM	Prison Militaire
RDC	République Démocratique du Congo
RMP	Registre du Ministère Public
RP	Registre de la Police
RSA	Rivest-Shanir-Aldman
SAAP	Section d'Appui à l'Administration Pénitentiaire
SGBD	système de Gestion des Bases des Données
SPC	Système Pénitentiaire Congolais
SP-CONNECT	Nom de l'application réalisée
SPP	Servitude Pénale Principale
SPS	Servitude Pénale Subsidiaire
SQL	Structured Query Language
TDEV	Temps de Développement
TF	Total Fonctionnel
UML	Unified Modeling Language
UP	Unified Process

Table des figures

1.1 Méthode UP 5
1.2 Diagramme1 Gantt des activités 7
1.3 Diagramme2 Gantt des activités 8

2.1 carte RDC avec 11 provinces 11
2.2 organigramme du SPC 16
2.3 organigramme du SPC 17

3.1 symboles utilisés dans la construction des cas d'utilisations 22
3.2 Cas d'utilisation «Effectuer les opérations pénitentiaires» 23
3.3 Cas d'utilisation «Gérer le dossier administratif du détenu» 26
3.4 Ministère de la justice 28
3.5 Cas d'utilisation «Recherche information» 29
3.6 symboles utilisés dans la construction du diagramme des classes 30
3.7 Diagramme des classes 31
3.8 symboles utilisés dans la construction du diagramme de déploiement 33
3.9 Diagramme de déploiement en local 34
3.10 Diagramme de déploiement en ligne 34

5.1 Interface d'illustration du cryptage RSA 48
5.2 Résultat du cryptage 49
5.3 Résultat du décryptage 49
5.4 Valeurs de paramètres RSA 50
5.5 Fichier Identifiant encrypté 52
5.6 Fichier Identifiant décrypté 53

6.1 Connexion 55
6.2 Interface d'accueil du Ministère de la justice 55
6.3 Tableau de bord du Ministère de la Justice 56
6.4 Interface d'accueil du greffier d'une prison 56
6.5 Interface d'enregistrement d'un nouveau prisonnier 57

6.6 Interface d'enregistrement des peines prononcées 57
6.7 Interface d'enregistrement du transfert d'un prisonnier 58
6.8 Interface d'enregistrement d'une sortie (libération) d'un prisonnier 58
6.9 Interface d'accueil du Directeur de prison 59
6.10 Interface d'enregistrement d'une hospitalisation du prisonnier 60
6.11 Interface d'enregistrement d'une visite 60
6.12 Interface d'affectation des prisonniers dans les cellules 61
6.13 Interface d'enregistrement des mesures disciplinaires 61
6.14 Interface d'accueil de l'administrateur du système 62
6.15 Billet de sortie 62
6.16 Interface-billet-de-sortie 63
6.17 Fiche d'identification d'un détenu 63
6.18 Interface d'impression de la fiche d'identification d'un détenu 64
6.19 Fiche des statistiques par prison 64
6.20 Interface d'impression des statistiques 65
6.21 Fiche de la population pénitentiaire globale 65
6.22 Interface d'impression des statistiques 66
6.23 Résultats de la recherche multi-critères 66
6.24 Contrôle de la capacité d'accueil des cellules 68
6.25 Interface de visualisation des candidats à la liberté conditionnelle 68

Liste des tableaux

2.1 Prisons par Province 10
2.2 Flux d'information 18
2.3 Description des postes de travail 19

3.1 Cas d'utilisation «se connecter» 24
3.2 Cas d'utilisation «Écrouer un prisonnier» 24
3.3 Cas d'utilisation «Gérer l'hospitalisation» 25
3.4 Cas d'utilisation «Effectuer une recherche multi-critère» 26
3.5 Cas d'utilisation «Effectuer la sortie d'un détenu» 27
3.6 Cas d'utilisation «Élaboration des rapports» 27
3.7 Cas d'utilisation «Amnistier un détenu» 28
3.8 Cas d'utilisation «suivi des cas irréguliers» 29

5.1 Valeur paramètre RSA 51

6.1 Valeurs paramètres COCOMO 70
6.2 Valeurs paramètres WebMo 71

RÉSUMÉ

La gestion du système pénitentiaire retrace toutes les activités et opérations effectuées au sein d'une prison par des agents qualifiés à ce service. Aujourd'hui, l'informatique est en plein essor grâce notamment à l'importance et à la place qu'elle crée dans la vie quotidienne. En effet, elle permet d'économiser le temps, de conserver et sécuriser les données tout en rehaussant la performance des prestations des institutions concernées.

En République Démocratique du Congo, avec l'accroissement du nombre de détenus dans les prisons pendant ces dernières décennies, le support d'information(registres) jadis utilisé n'est plus à même de répondre efficacement aux différentes sollicitations. De plus, le personnel pénitentiaire, étant lui-même insuffisant, non professionnel, corrompu, accuse un retard notoire en matière de NTIC dans l'accomplissement de leurs tâches quotidiennes.

Par conséquent, il s'observe beaucoup de situations irrégulières dans l'arrestation et la détention des détenus. Notre objectif, dans le cadre de ce projet de fin d'étude de master, se propose de mettre en place une application informatique sécurisée pour la gestion du système pénitentiaire afin d'améliorer la qualité des services rendus par le personnel pénitentiaire et ceci, dans les normes requises de la justice congolaise.

Ainsi, notre solution permettra au ministère de la justice, au personnel pénitentiaire, aux avocats, de relever tous les cas d'irrégularités, d'éditer automatiquement différents rapports, de signaler tous les détenus à libérer conditionnellement, de rechercher les informations sur le détenu, de prévoir à tout point d'échéance une sortie éventuelle des prisonniers, etc.

Pour mener à bien notre étude, nous avons utilisé la méthode UP pour la conception du système et le programmé avec des outils tels que Php-mysql,javascript, ajax.
L'application informatique réalisée est un site web dynamique sécurisé et hébergé donnant un espace de travail à toutes les prisons de la RDC.

Mots clés : Système pénitentiaire, application informatique, Sécurité informatique, RDC

ABSTRACT

The management of the penitentiary system traces all the activities and operations carried out within a prison by officers qualified in this service. Today, IT is booming thanks in particular to the importance and place it creates in everyday life. Indeed, it saves time, preserves and secures data while improving the performance of the services of the institutions concerned.

In the Democratic Republic of Congo, with the increase in the number of prisoners in prisons over the past decades, the information medium (registers) previously used is no longer able to respond effectively to the various requests. In addition, the prison staff, being themselves insufficient, unprofessional, corrupt, are notoriously behind in terms of NICT in the accomplishment of their daily tasks.

Hence, many irregular situations can be observed in the arrest and detention of detainees. Our objective, within the framework of this final master's study project, is to set up a secure computer application for the management of the prison system in order to improve the quality of the services provided by the prison staff and this, in the standards required of Congolese justice.

Thus, our solution will allow the Ministry of Justice, prison staff, lawyers, to identify all cases of irregularities, to automatically edit various reports, to report all detainees to be released on parole, to search for information on the detainee. , to foresee at any point of expiry a possible release of prisoners, etc.

To carry out our study, we used the UP method for the design of the system and programmed it with tools such as Php-mysql, javascript, ajax.
The computer application produced is a secure and hosted dynamic website giving a workspace to all the prisons in the DRC.

Keywords : Prison system, IT application, IT security, DRC

Table des matières

IDENTIFICATION DES MEMBRES DU JURY i
DEDICACES ii
REMERCIEMENTS iii
SIGLES ET ABREVIATIONS iv
LISTE DES FIGURES vi
LISTE DES TABLEAUX vii
RESUME viii
ABSTRACT ix
AVANT-PROPOS xiv
INTRODUCTION GENERALE 1
CHAPITRE 1 – PRÉSENTATION DU PROJET DE RECHERCHE 2
1.1 Contextualisation et actualité du projet de recherche 2
1.2 Objectif du projet 3
1.2.1 Objectif global 3
1.2.2 Objectifs spécifiques 3
1.3 Problématique 3
1.4 Solutions proposées 4
1.5 Résultats attendus 4
1.6 Apports scientifiques et technologiques 4
1.7 Domaines d'application 5
1.8 Méthodologie 5
1.9 Outils mathématiques et plateforme de conception et de développement 6
1.10 Chronologie des activités du projet 6
1.11 Conclusion au chapitre sur la présentation du projet 6
CHAPITRE 2 – ÉTUDE ET ANALYSE DU SYSTÈME EXISTANT 9
2.1 Introduction 9

2.2 Structure organisationnelle et fonctionnelle du SPC 9
2.2.1 Quelques définitions 9
2.2.2 Établissements pénitentiaires en RDC 10
2.2.3 Architecture du Système Pénitentiaire Congolais 10
2.2.4 Contrôle des prisons et des maisons d'arrêt 11
2.2.5 Personnel des prisons et des maisons d'arrêt 12
2.2.6 Personnel de surveillance 12
2.2.7 Personnel éducatif 12
2.2.8 Admission des détenus dans les prisons et maisons d'arrêt 12
2.2.9 Répartition des détenus dans les locaux de détention 13
2.2.10 Libération conditionnelle 13
2.2.11 Évasions au sein des prisons 13
2.3 Quelques anomalies du Système pénitentiaire Congolais 14
2.3.1 Anomalie liée à l'accès aux données 14
2.3.2 Anomalie liée aux contrôles réguliers 14
2.3.3 Anomalie liée au personnel 14
2.3.4 Anomalie liée à la répartition des détenus dans les cellules 15
2.3.5 Anomalie liée à la durée de détention des détenus 15
2.3.6 Anomalie liée à l'utilisation de la liberté conditionnelle 15
2.4 Modélisation Métier 15
2.4.1 Structure organisationnelle d'une prison 15
2.4.2 Missions du service pénitentiaire 16
2.4.3 Diagramme de flux d'information général 16
2.4.4 Étude des postes 17
2.5 Analyse des procédures de travail 17
2.6 Conclusion au chapitre d'analyse de l'existant 20
CHAPITRE 3 — CONCEPTION DU NOUVEAU SYSTÈME A L'AIDE D'UML 21
3.1 Présentation du langage UML 21
3.1.1 Introduction 21
3.1.2 Diagrammes d'UML 21
3.2 Modélisation du système 22
3.2.1 Diagramme de cas d'utilisation 22
3.2.2 Identification des Diagramme de cas d'utilisation du système conçu 23
3.2.3 Diagramme des classes 29
3.2.4 Construction du diagramme de classe 31

3.3 Modèle Logique des données du nouveau système 31
3.3.1 Règles de passage du diagramme de classes au modèle logique 31
3.3.2 Élaboration du modèle logique 32
3.3.3 Diagrammes de déploiement 32
3.3.4 Construction du diagramme de déploiement 33
3.4 Conclusion au chapitre sur la conception du système 35
CHAPITRE 4 — MODÈLE MATHÉMATIQUE UTILISE POUR LA RÉALISATION DES REQUÊTES 36
4.1 Introduction 36
4.2 Modèle Relationnel 36
4.2.1 Définition, historique et évolution 36
4.2.2 Justification du choix de ce modèle 37
4.2.3 Opérateurs de l'algèbre relationnelle 37
4.2.4 Fonctions d'agrégat en Algèbre Relationnelle 38
4.2.5 Règles de réécriture 39
4.2.6 Conception de nos requêtes en Algèbre Relationnelle 39
4.3 Conclusion au chapitre sur le modèle mathématique 43
CHAPITRE 5 — SÉCURISATION DU NOUVEAU SYSTÈME DE GESTION DU SYSTÈME PÉNITENTIAIRE DE LA RDC 44
5.1 Introduction 44
5.2 Objectifs de la sécurité 44
5.3 Mécanismes de sécurité 45
5.4 Cryptographie 45
5.4.1 Introduction 45
5.4.2 Historique 46
5.4.3 Types de cryptographie 46
5.5 Cryptographie par RSA 46
5.5.1 Usages de RSA 47
5.5.2 Description de l'algorithme RSA 47
5.5.3 Exemple d'application 47
5.5.4 Quelques failles de RSA 47
5.5.5 Application de l'algorithme RSA-Optimal Asymmetric Encryption Padding dans notre projet 48
5.5.6 Données Test 50
5.6 Conclusion au chapitre sur la sécurisation du nouveau système 53

CHAPITRE 6 – PRÉSENTATION DU FONCTIONNEMENT DE L'APPLICATION 54

6.1 Introduction 54
6.2 Connexion 54
6.3 Analyse par acteur 55
6.3.1 Ministère de la Justice 55
6.3.2 Greffier de la prison 56
6.3.3 Directeur de la prison 58
6.3.4 Administrateur du système 61
6.4 Génération des rapports 62
6.4.1 Billet de sortie 62
6.4.2 Fiche d'identification d'un détenu 63
6.4.3 Statistiques par prison 64
6.4.4 Population pénitentiaire globale 65
6.5 Résultats principaux et discussions 65
6.5.1 Par rapport au problème d'irrégularité 66
6.5.2 Par rapport au problème de la recherche d'information 66
6.5.3 Par au problème d'accès aux données en temps réel 67
6.5.4 Par rapport à l'élaboration des rapports 67
6.5.5 Par rapport problème de surpopulation dans les prisons 67
6.5.6 Par rapport au problème de la non possibilité de demande de la liberté conditionnelle 67
6.5.7 Sécurité 68
6.6 Processus d'hébergement du projet SP-CONNECT 69
6.6.1 Introduction 69
6.6.2 Présentation de la technique d'hébergement 69
6.6.3 Procédure pour mettre en ligne SP-Connect 69
6.7 Coût du logiciel 70
6.7.1 Méthode COnstructive COst MOdeL 70
6.7.2 Méthode COCOMO II 71
6.7.3 Méthode WebMo 71
6.7.4 Calcul du Coût de notre projet avec WebMo 71
6.8 Conclusion au chapitre sur la présentation de l'application 72

CONCLUSION 73

RECOMMANDATIONS 74

BIBLIOGRAPHIE 75

AVANT-PROPOS

Ce mémoire rentre dans le cadre de l'obtention du diplôme de Master en Génie Informatique à l'Université du Burundi. Il étudiera la mise en place d'une application informatique sécurisée pour la gestion du système pénitentiaire de la république démocratique du Congo. L'idée de ce mémoire de recherche est venue du constat des irrégularités liées aux arrestations et détentions arbitraires dans les maisons de détentions en République démocratique du Congo.

En effet, pendant ces dernières décennies, le support d'information (registres) utilisé dans les prisons n'est plus à même de répondre efficacement aux différentes requêtes. De plus, le personnel pénitentiaire, étant lui-même insuffisant, non professionnel, corrompu, accuse un retard notoire en matière de NTIC dans l'accomplissement de leurs tâches quotidiennes. Par conséquent, il s'observe beaucoup de situations irrégulières dans l'arrestation et la détention des détenus.

Cette étude se veut être une contribution à l'amélioration de la qualité des services rendus par le personnel pénitentiaire et ceci, dans les normes requises de la justice congolaise. A titre illustratif, notre solution permettra au ministère de la justice, au personnel pénitentiaire, aux avocats, de relever tous les cas d'irrégularités, d'éditer automatiquement différents rapports, de signaler tous les détenus à libérer conditionnellement, de rechercher les informations sur le détenu, de prévoir à tout point d'échéance une sortie éventuelle des prisonniers, de suivre à distance toutes les incarcérations effectuées à l'échelle nationale etc.

Des difficultés n'ont pas manqué. Elles concernent particulièrement la disponibilité de certains matériels informatiques pour le montage du protype de ce présent système. Il s'agit de la carte Raspberry, qui devrait nous aider à réaliser notre propre serveur. Cette dernière situation nous a obligé d'opter pour une solution d'hébergement par une entreprise informatique.

INTRODUCTION GENERALE

Plusieurs rapports[2][4][3] alarmants sur la situation des prisonniers dans les prisons congolaises ont vu le jour pendant ces deux dernières décennies. La surpopulation, les mauvaises conditions de détention, le manque criant d'un personnel qualifié sont parmi les maux cités. [1] déclare par exemple dans sa thèse de maîtrise que la moyenne de surpopulation des prisons est de 260%. Cette surpopulation est la principale cause d'une gestion pénitentiaire calamiteuse basée sur des supports des données inappropriés comme des registres ou cahiers simples.

Avec l'avènement du numérique, toutes les entreprises et sociétés s'orientent vers l'automatisation de l'ensemble de ses tâches. C'est ainsi qu'il est pertinent de s'intéresser à une étude qui vise à informatiser l'ensembles d'activités et tâches liées au système pénitentiaire congolais. La mise en place d'un système d'information d'une société est l'un des thèmes traités en master Sciences de l'ingénieur à l'Université du Burundi.

La lecture des différents rapports sur la gestion du système pénitentiaire congolais a soulevé des questionnements qui m'ont interpellé et attiré mon intérêt pour apporter ma contribution tant soit peu en vue d' assister cette population misérable et souffrante. Des travaux ont été mené pour améliorer le bon fonctionnement du système pénitentiaire congolais. Une série de recommandations a été formulée parmi lesquelles nous pouvons citer :

- L'application du principe de la liberté conditionnelle en vue de permettre une libération d'un bon nombre des détenus et ainsi diminuer la population carcérale ;
- La mise sur pied d'un comité de contrôle sur la régularité des dossiers de chaque détenu ;
- La mise en application de la politique de grâce, d'amnistie etc. à l'échelle nationale ;
- La publication dans le journal officiel des jugements rendus par rapport à chaque infraction pour souci de conformité des peines au niveau national ;
- etc.

Malgré ces bonnes recommandations qu'on retrouve dans le code pénal, proposé dans ces travaux, bon nombres restent toujours inappliqués jusqu' aujourd'hui. En effet, d'une part la plupart des prisons utilise un système manuel avec un personnel non qualifié et non motivé, ne maîtrisant pas toutes ces lois. D'autre part, les supports des données utilisés ne facilitent pas non plus la tâche pour l'exécution de ces dernières. Dans le cadre de cette thèse, nous nous intéressons à la problématique de rendre tous ces traitements automatisables sur un support informatique constituant la plaque tournante de toutes les données du système pénitentiaire congolais.

Afin de traiter le sujet et de répondre aux questionnements émis, un plan de recherche a été établi. Tout d'abord, nous avions effectué une descente sur quelques prisons. Nous avions eu des entretiens directs avec le personnel et quelques juristes. La recherche empirique a été complétée par de nombreuses lectures sur le sujet. Nous voudrions mettre en place une application informatique qui faciliterait l'automatisation de tous les traitements du système pénitentiaire avec une possibilité d'avoir une base des données unique à l'échelle nationale.

Chapitre 1

PRÉSENTATION DU PROJET DE RECHERCHE

1.1 Contextualisation et actualité du projet de recherche

Depuis l'antiquité à nos jours, l'homme a toujours essayé d'inventer des outils qui lui facilitent à compter, traiter et stocker de l'information. L'invention des nombres, des systèmes d'énumérations, des automates, des calculatrices, des ordinateurs etc en sont des exemples illustratifs. Actuellement, les ordinateurs ne sont non seulement capables de stocker de grosses quantités d'informations mais aussi sont équipés des programmes capables de structurer et manipuler efficacement ces données.

Dans toutes les prisons de la RDC, la plupart n'utilise pas un système informatique pour la gestion de ses données. Or, dans le contexte mondial actuel, aucun n'organisme ne pourrait ignorer le rôle et la place des NTIC dans la maîtrise, la concurrence et l'amélioration des services. Cet usage s'avère un moyen pour le partage en temps réel des informations entre plusieurs utilisateurs distants, l' augmentation des performances dans la recherche d'information dans cette masse des données et l'atteinte des objectifs fixés dans les délais impartis.

Le non usage des NTIC est devenu un handicap pour l'exécution d'une justice équitable au sein des prisons et toute une série des maux. Dans les prisons, il est à noter plusieurs difficultés comme le témoigne aussi le dernier rapport de la MONUSCO dans [2].

Premièrement, il n'existe aucun mécanisme de signalisation des sorties dues à l'expiration de peine ou au dépassement de délai préventif.
Deuxièmement, la recherche d' informations n'est pas chose aisée étant donné qu'il n'existe pas des techniques de recherches efficaces adaptées au support papier.
Troisièmement, l'attribution des cellules s'effectuent aléatoirement sans aucune information sur la situation particulière de chacune des cellules.
Quatrièmement, lors d'une visite, retrouver l'adresse de la cellule d'un prisonnier n'est pas non plus facile.
Cinquièmement, certaines pratiques jadis exigées sont même abandonnées, comme par exemple la cotation régulière de conduite.
Sixièmement, l'élaboration des rapports se faisant manuellement nécessite beaucoup de temps

car obligeant d'abord la recherche information.

En fin, les prisons n'étant pas en mesure de se partager des informations en temps réel, la police ou le Président de République par exemple, se trouve en difficulté de prendre de bonnes décisions respectivement en matière de l'octroie des casiers judiciaires et de la politique des mesures de grâces,d'amnistie etc.

1.2 Objectif du projet

1.2.1 Objectif global

L'objectif est de concevoir une application modélisant le système pénitentiaire congolais qui permettra grâce à une base de données d'automatiser ses différentes activités depuis l'entrée jusqu'à la sortie d'un prisonnier de la prison.

1.2.2 Objectifs spécifiques

1. Concevoir une base de données informatique pour la sauvegarde des données sur les prisonniers ;
2. Repérer automatiquement et facilement tous les prisonniers répondant à un profil précis ;
3. Alerter toutes les irrégularités par rapport aux règlements du système pénitentiaire ;
4. Attribuer une note de conduite à un prisonnier ;
5. Créer un module de gestion des cellules ;
6. Partager des données et informations des prisonniers entre prisons ;
7. Générer automatiquement des rapports sur les statistiques par prison ;
8. Aider dans la prise de décision en rapport avec l'octroie de casier judiciaire et la liberté conditionnelle ;
9. Archiver électroniquement des données et documents y relatifs ;
10. Concevoir un module de gestion des visites ;
11. Sécuriser et contrôler l'accès aux données.

1.3 Problématique

1. La difficulté à retrouver des prisonniers détenus illégaux par rapport à l'expiration de peine ou ayant dépassé largement la durée de détention provisoire ;
2. La recherche des prisonniers répondant à un profil (ensemble des critères)prend beaucoup de temps puisqu'elle se fait manuellement ;
3. L'identification de la cellule à affecter un prisonnier est élaborée aléatoirement et pourtant il y a une surpopulation ;
4. La cotation de conduite ne se fait plus, alors qu'utile lors de la demande d'une liberté conditionnelle ;
5. L'octroie du casier judiciaire par la police élaboré sans aucune information sur l'individu ;

6. La difficulté à repérer des cas récidivistes ;
7. Politique d'amnistie, de grâce présidentielle difficilement mis en œuvre car les données ne sont pas centralisées ;
8. La difficulté d'élaborer les statistiques par prison en temps réel ;
9. La sécurité et la protection des données sont faibles.

1.4 Solutions proposées

1. Signalisation automatique des détenus à libérer ;
2. Recherche automatique basée sur langage SQL ;
3. Calcul automatique de la cellule la moins peuplée ;
4. Cotation de conduite automatisée ;
5. Mise en réseau des données des différentes prisons ;
6. Module d'aide à la prise de décision en matière de liberté conditionnelle et octroi des casiers judiciaires ;
7. Génération automatique des rapports ;
8. Application de l'algorithme RSA et césar pour la sécurité et la protection des données ;

1.5 Résultats attendus

1. Diminution des cas des détenus étant dans une situation irrégulière ;
2. Répartition optimisée des détenus dans différentes cellules ;
3. Rapports et statistiques des différentes prisons obtenus dans un bref délai ;
4. Disponibilité en temps réel des informations recherchées sur les détenus ;
5. Obtention d'un fichier unique des données sur les individus à suivre par la police au niveau national ;

Toutes ces solutions envisagées ici vont concourir à l'exécution rapide, conforme, juste et sans beaucoup de peine de toutes les tâches pénitentiaires exécutées par le personnel de prison et à la facilitation d'accès aux informations à tous les acteurs de l'appareil judiciaire pour le suivi des dossiers. Par conséquent, la qualité des services se retrouverait améliorée ainsi que l'efficacité des agents dudit service dans sa globalité. Tout en facilitant l'automatisation de différentes tâches pénitentiaires, cette application diminuera, de plus, le nombre cas des détentions irrégulières. Ensuite, elle supprimera la file d'attente des visiteurs recherchant diverses informations sur les prisonniers, qui éventuellement causé par l'approche manuel. En fin, elle renforcera le suivi du contrôle du dossier de chaque détenu, qui une fois archaïque, il peut être source de l'injustice[2].

1.6 Apports scientifiques et technologiques

1. Proposition d'une approche de déploiement d'une base des données repartie ;
2. Module de répartition optimisée des cellules dans une prison ;
3. Techniques et algorithmes de création des Rapports ;
4. Usage de l'algorithme de RSA dans la sécurisation de l'application ;
5. Usage de la technologie MVC dans la construction de l'application web ;

1.7 Domaines d'application

1. Entreprises multi-sites avec la nouvelle approche de traitement de base des données reparties ;
2. Police avec le suivi des récidivistes.

1.8 Méthodologie

Nous allons utiliser la méthodologie UP pour mettre en place ce système. Les différentes étapes de cette méthode nous seront toutes utiles pour identifier les besoins des utilisateurs et les fonctionnalités du futur système[8]. Nous aurons à produire tour à tour un diagramme de classe, un diagramme de cas d'utilisation, un diagramme de déploiement, etc. Bien entendu cette étape est précédée par une phase d'analyse du système manuel et des documents. Le Processus unifié est une méthode de développement logiciel [11] :
- basé sur le langage UML ;
- piloté par des cas d'utilisations ;
- centré sur l'architecture ;
- caractérisé par une approche itérative et incrémentale.

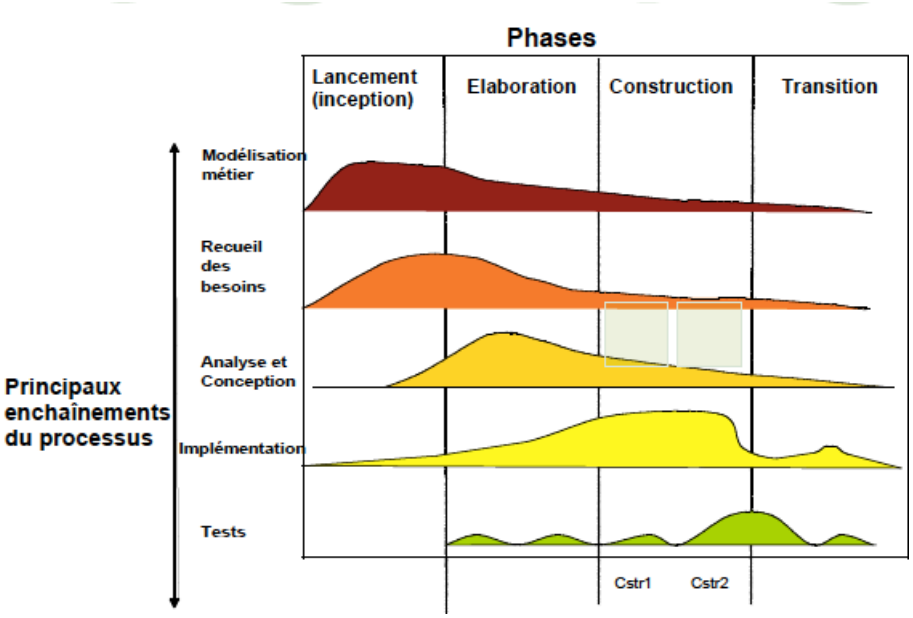


FIGURE 1.1 – Méthode UP

Comme le montre la Figure 1.1, la méthode UP comprend quatre grandes phases. Il s'agit de :
- Phase de démarrage : C'est la phase où on définit l'objectif du projet et identifie tous les acteurs et les cas d'utilisations essentiels. Cette phase a été réalisée au chapitre 1 du présent travail.
- Phase d'élaboration : Elle permet d'avoir une bonne connaissance des besoins et d'établir une base de l'architecture. Nous allons réaliser l'architecture de notre système en utilisant les différents diagrammes d'UML.
- Phase de construction : Il s'agit du développement du produit en plusieurs itérations(3 à 5 pour un projet complexe) pour une version bêta.
- Phase de transition : Cette phase consiste à préparer le produit pour l'utilisateur final,formation, installation, support,... Dans chaque phase, il y a des activités à réaliser. Les principales activités pendant le développement d'un logiciel sont :

- Expression des besoins(modélisation métier) : Il est question de modéliser les possibilités du système et besoins utilisateurs. Autrement dit, pendant cette activité on expose les cas d'utilisation et leurs relations avec les utilisateurs
- Analyse(modélisation des besoins) : Il s'agit de la modélisation du système et des besoins détaillés des utilisateurs. Les cas d'utilisations sont détaillés et on obtient une première répartition du comportement du système sur divers objets.
- Conception : Cette activité permet de définir la structure statique du système sous forme de sous système, classes et interfaces. Elle définit aussi les cas d'utilisations réalisés sous forme de collaborations entre les sous systèmes, les classes et interfaces.
- Implémentation : Cette activité permet de mettre en œuvre les composants (code source). C'est à dire réaliser par la programmation les différents composants du système.
- Tests : Elle concerne la vérification du système dans son ensemble. C'est à dire on décrit les cas de test vérifiant les cas d'utilisations.

Enfin, il est à noter que sur cette figure qu'en phase de lancement, une plus grande partie du temps sera consacré à l'analyse des besoins qu'aux tests ; inversement en phase de transition, les tests sont encore en cours alors que l'analyse de besoin et son raffinage sont théoriquement bouclés depuis la phase de construction.

1.9 Outils mathématiques et plateforme de conception et de développement

- Algèbre relationnelle ;
- Fonctions d'agrégats SQL
- Langage UML ;
- PHP-MYSQL du coté serveur ;
- HTML,JAVASCRIPT,CSS,AJAX du coté client ;

1.10 Chronologie des activités du projet

Définition 1.1 *Un projet est un ensemble d'activités organisées en phases ou étapes et formant l'unité de gestion permettant la réalisation d'un objectif défini et précis.*

Autrement dit, c'est une opération ponctuelle ayant un début et une fin, nécessitant la mise en œuvre de ressources humaines et matérielles pour sa réalisation.

Notre projet de fin d'étude étant aussi un projet au sens propre du terme, a été réalisé sur base des activités suivantes que nous représentons grâce au diagramme de Gantt, couramment utilisé en gestion de projet.
Un diagramme de Gantt répertorie toutes les tâches à accomplir pour mener le projet à bien, et indique la date à laquelle ces tâches doivent être effectuées (le planning).

1.11 Conclusion au chapitre sur la présentation du projet

De ce qui précède, il est clair que l'exécution des tâches dans le SPC pose de sérieux problèmes. Dans ce chapitre, nous avions conçu un projet informatique pour remédier aux maux qui gangrènent le bon fonctionnement des activités du SPC. En vue d'atteindre ce dernier objectif, une

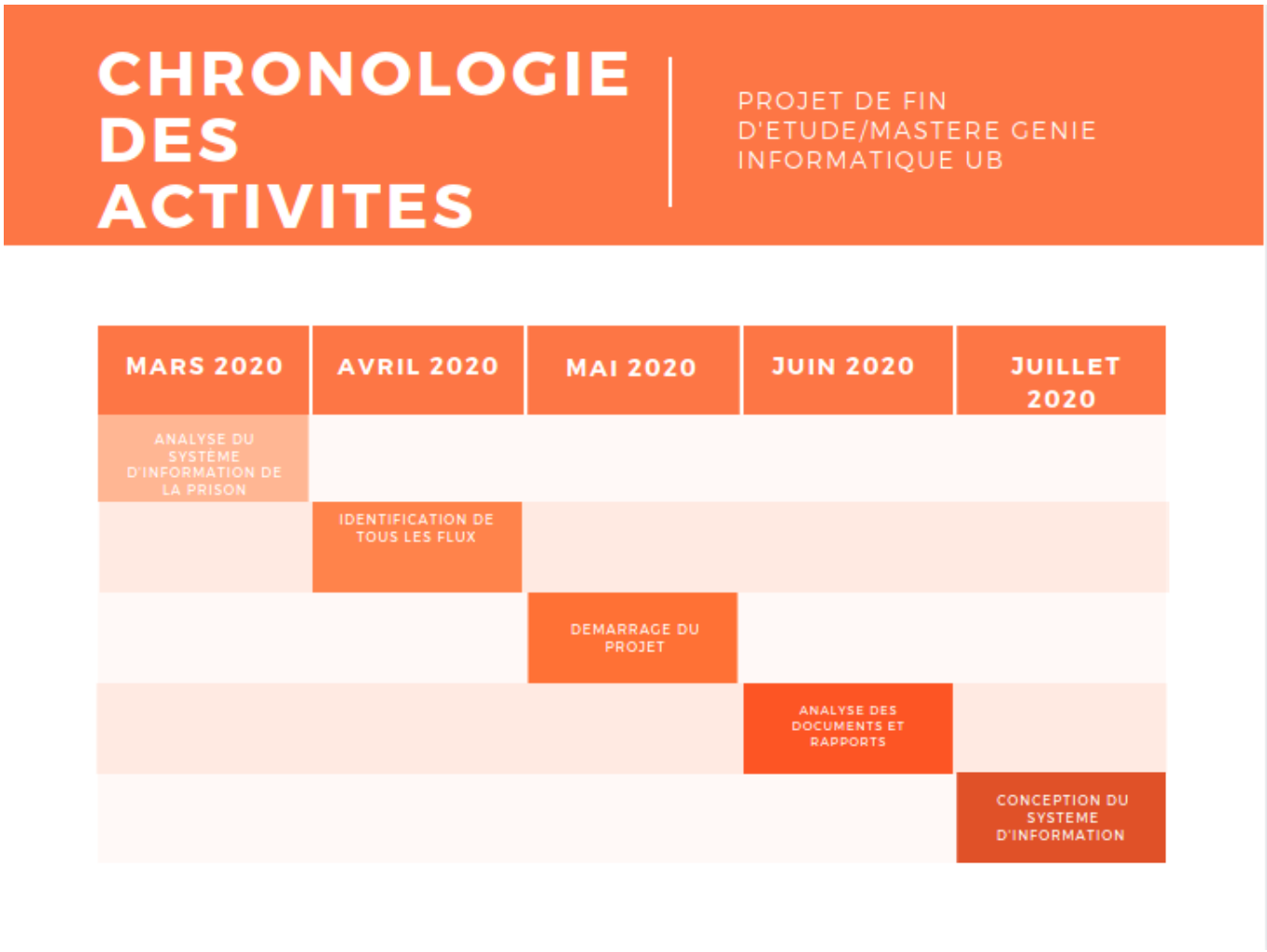


FIGURE 1.2 – Diagramme1 Gantt des activités

planification des activités du projet s'est avérée indispensable. C'est pourquoi nous finissons cette partie par la présentation du diagramme de Gantt des activités que nous avions menés. Il est à signaler que le présent projet est réalisé dans un cadre de projet de fin d'étude. D'où une contrainte sur son délai d'exécution ainsi qu' une limitation sur les ressources matérielles et financières à allouer.

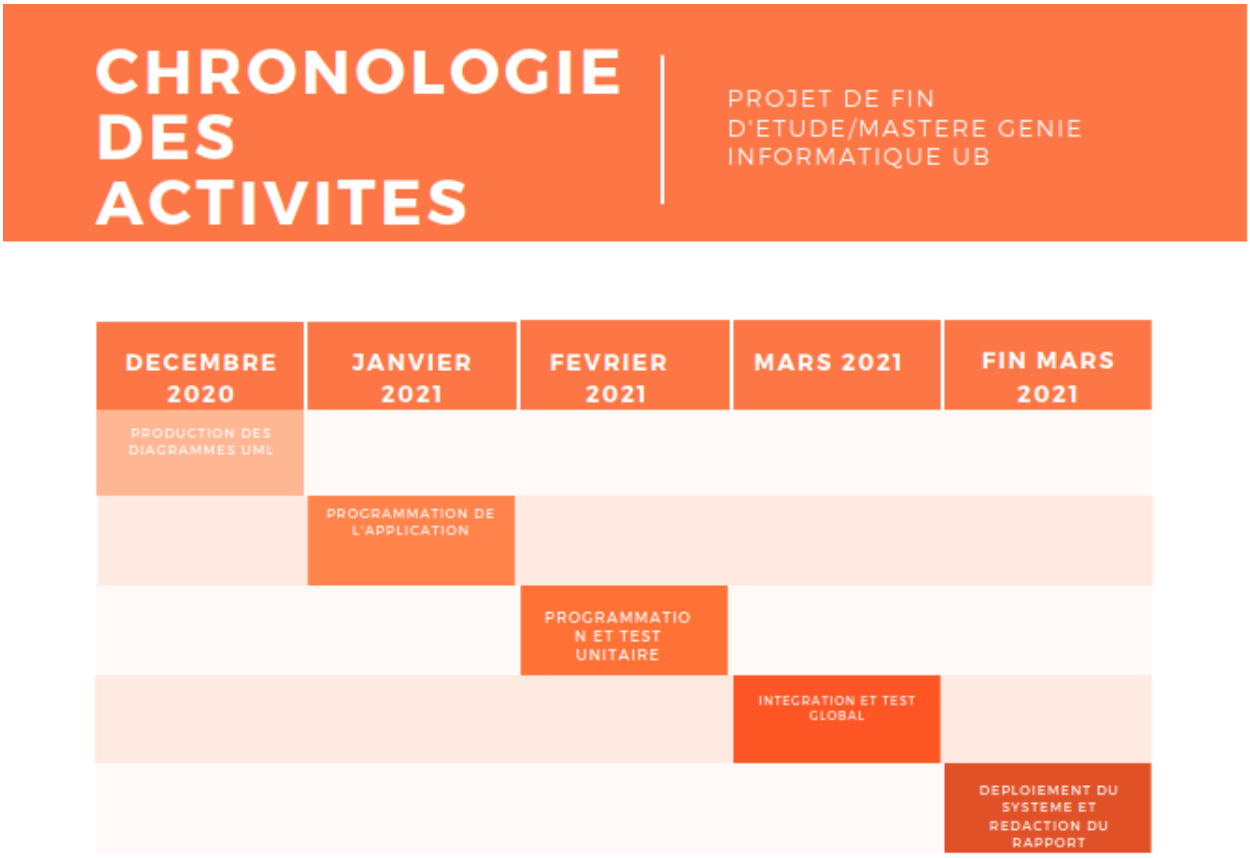


FIGURE 1.3 – Diagramme2 Gantt des activités

Chapitre 2

ÉTUDE ET ANALYSE DU SYSTÈME EXISTANT

2.1 Introduction

Avant que le malade ne soit soigné par le médecin, celui-ci se présente tout d'abord en lui fournissant son identité et ce qu'il sent. Ensuite le médecin diagnostique ce qui ne va pas et enfin lui propose un remède. C'est ainsi que ce chapitre présente le système pénitentiaire congolais sous l'angle organisationnel et opérationnel à la première section. Il détecte ensuite les failles de l'état des lieux de ce système à la deuxième section et finit par une modélisation métier du système à concevoir.

2.2 Structure organisationnelle et fonctionnelle du SPC

2.2.1 Quelques définitions

Définition 2.1 *Un système pénitentiaire est formé par l'ensemble des prisons où sont détenues les personnes avant leur procès et celles qui ont été condamnées à des peines de prison.*

On distingue, selon les caractéristiques des détenus, les maisons d'arrêt, les centres de détention et les maisons centrales. Les catégories des détenus sont :

Définition 2.2 *Un détenu prévenu est une personne emprisonnée qui n'a pas encore été jugée, contre laquelle est exercée l'action publique devant une juridiction de jugement en matière correctionnelle et contraventionnelle.*

Définition 2.3 *Un détenu condamné est une personne ayant fait l'objet d'une décision de condamnation à l'emprisonnement ferme, ayant acquis un caractère définitif.*

Ainsi on a :

Définition 2.4 *Les maisons d'arrêt, où sont incarcérés les individus placés en détention provisoire(avant leur procès) et les personnes condamnées à un an de prison maximum.*

Définition 2.5 *Les maisons centrales, réservées aux personnes condamnées aux peines de longue durée.*

Définition 2.6 *Les centres de détention, qui accueillent des condamnés à des peines de longue durée arrivant à la fin de leur peine.*

Des situations particulières peuvent conduire à la libération d'un détenu. C'est notamment le cas d'une libération conditionnelle, d'une mesure d'amnistie,etc.

2.2.2 Établissements pénitentiaires en RDC

En RDC, les prisons comprennent :
- les prisons centrales ;
- les prisons de district ;
- les prisons de police ou cachot.

Au siège de chaque tribunal de première instance se trouve une prison centrale, des prisons de district dans chaque localité où un tribunal de district a son siège habituel, à l'exclusion des localités où est établie une prison centrale. Il est établi en annexe à chacune des prisons, une maison d'arrêt. Voici la cartographie des prisons en République démocratique du Congo, réalisée en Août 2013 par la Section d'Appui à l'Administration Pénitentiaire SAAP de la MONUSCO[1] :

Table 2.1 – Prisons par Province

Provinces	P.C	CDD	PDP	PDD	PM	MAA	Total	TF	NF
BANDUNDU	1	1	14	5	0	0	21	14	7
BASCONGO	1	1	7	3	1	0	13	7	6
EQUATEUR	1	1	28	6	1	0	37	19	18
KASAI-O	1	0	8	3	0	0	12	9	3
KASAI-OR	1	0	9	3	0	0	13	9	4
KATANGA	1	1	21	5	0	2	30	20	10
KINSHASA	1	0	0	0	1	0	2	2	0
MANIEMA	1	1	7	0	0	21	30	8	22
NORD-KIVU	1	1	6	0	0	3	11	5	6
PROVINCE- O	1	2	32	3	0	0	38	16	22
SUD-KIVU	1	0	18	0	0	1	20	11	9
Total	11	8	150	28	3	27	227	120	107

Ces provinces se présentent de la manière suivante, selon la Figure 1.1. Pour rappel, la superficie de la RDC est de 2.345 millions km2 avec 84.07 millions d'habitants en 2018. Et Selon le dernier rapport[7] sur les statistiques de la population pénitentiaire de 2015, le nombre des détenus avoisinait 16.500 individus en RDC.

2.2.3 Architecture du Système Pénitentiaire Congolais

La configuration administrative telle que prévue par l'Ordonnance [5], laisse apparaître l'existence des Sections d'inspection des établissements pénitentiaires dans chaque chef-lieu de province. Ces sections placées sous l'autorité directe du Ministre de la Justice, fonctionnent comme

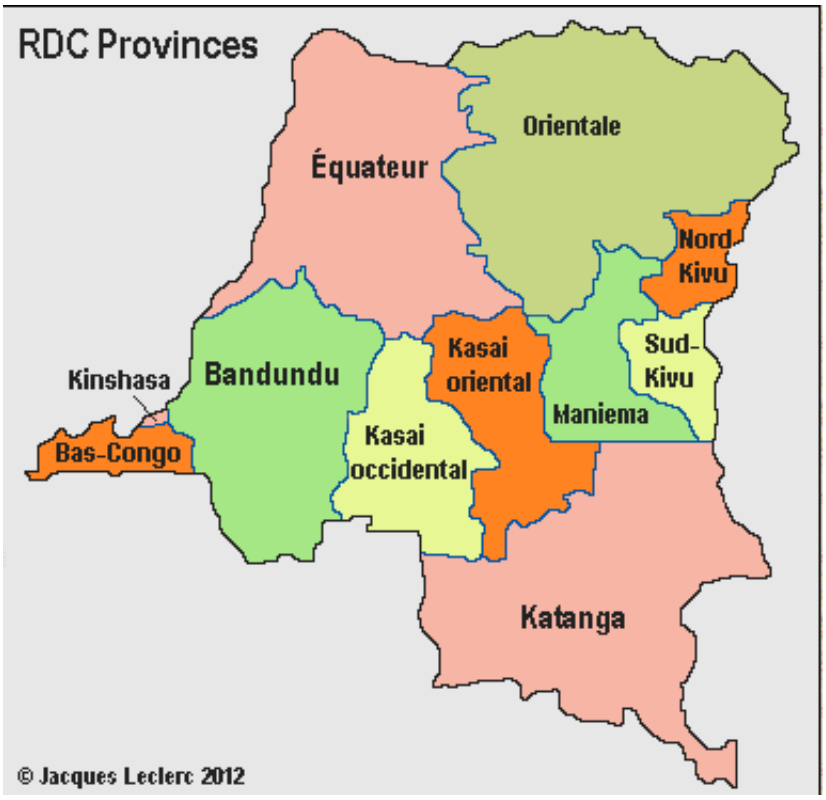


FIGURE 2.1 – carte RDC avec 11 provinces

des entités indépendantes les unes des autres. La Direction des Services Pénitentiaires en tant que structure centrale assure la coordination de l'ensemble des activités du système pénitentiaire de la RDC. Elle s'appuie sur un organigramme comprenant des Divisions et des Bureaux au niveau central, un Bureau rattaché à une Division au niveau provincial et des établissements pénitentiaires répartis à travers le territoire national.

2.2.4 Contrôle des prisons et des maisons d'arrêt

L'inspecteur territorialement compétent chargé de la direction de la section d'inspection des établissements pénitentiaires visite les prisons, les maisons d'arrêt et les camps de détention au moins une fois par trimestre telle que prévue par l'ordonnance [5]. Il vérifie les registres d'écrou, le registre d'hébergement et s'assure si aucune personne arrêtée n'est retenue au-delà du temps nécessaire pour être conduite devant l'autorité judiciaire compétente pour exercer les poursuites. En outre, il contrôle la tenue du dossier personnel du détenu.

Signalons en outre, que le gouverneur de province, l'officier du ministère public ainsi qu'un médecin désigné par le gouvernement visite régulièrement les établissements pénitentiaires. Les visiteurs consignent leurs observations dans le registre spécial conservé par le gardien et dressent un rapport qu'ils envoient à leur supérieur hiérarchique ainsi qu'à l'inspecteur des établissements pénitentiaires, lequel le transmet avec ses avis et considérations au ministre de la Justice du gouvernement central.

2.2.5 Personnel des prisons et des maisons d'arrêt

Au niveau des établissements pénitentiaires, nous retrouvons le personnel de garde et d'administration, le personnel de surveillance et le personnel éducatif des établissements pénitentiaires qui est placé sous la direction et la surveillance de l'inspecteur territorialement compétent chargé de la direction de la section d'inspection des établissements pénitentiaires. L'organisation interne des prisons et maisons d'arrêt est régie par la loi du 31 mars 1987 qui dispose qu'il doit exister dans chaque prison et maison d'arrêt un comité de gestion chargé d'administrer la prison. Ce comité est composé du directeur de prison, de son adjoint et de deux administrateurs. Le directeur coordonne et supervise l'ensemble. Il dispose du pouvoir de refuser l'incarcération d'un détenu si les titres prévus aux articles 30 et 34 de l 'ordonnance numéro 344 du 17 septembre 1965 ne lui sont pas présentés. Chaque prison, maison d'arrêt y annexée, et chaque camp de détention est gardé et administré par un gardien(directeur de prison) ayant le rang de chef de bureau, et désigné par le ministre de la Justice du gouvernement central, ou par son délégué parmi le personnel du cadre des services pénitentiaires. Le gardien est chargé :

1. de régler les détails de service de la prison, de la maison d'arrêt y annexée ou du camp de détention ;
2. d'assurer la garde des détenus et le maintien de l'ordre et de la discipline ;
3. de tenir les diverses écritures dans les registres d'écrou,memento, des sanctions etc. ;
4. d'assurer la conservation des documents visés à ces articles et, d'une manière générale, de tenir les archives de la prison, de la maison d'arrêt y annexée ou du camp de détention ;
5. d'assurer la conservation des biens visés à l'article 32, ainsi que des vivres, du matériel et des fournitures.

2.2.6 Personnel de surveillance

La surveillance immédiate des détenus est exercée par les surveillants. Dans les prisons, maisons d'arrêt ou camps de détention où il n'est pas possible de placer des surveillants ou d'en placer en nombre suffisant, la surveillance est exercée par des gendarmes, des agents de la police nationale ou de la police provinciale.

2.2.7 Personnel éducatif

L'éducation immédiate des détenus est assurée par des instructeurs. Le gardien peut charger les surveillants qui y sont aptes, des fonctions d'éducateurs.

2.2.8 Admission des détenus dans les prisons et maisons d'arrêt

Le gardien ne peut procéder à l'incarcération d'un détenu dans une prison ou dans un camp de détention que sur présentation d'un des titres suivants :

1. Une réquisition en exécution des jugements ou arrêts émanant soit du ministère public, soit du juge lorsque celui-ci a siège sans l'assistance du ministère public ;
2. Une réquisition en exécution d'un jugement rendu par un tribunal coutumier, ou un extrait d'un tel jugement.

3. Une décision du tribunal ordonnant l'internement d'un vagabond ou d'un mendiant mis à la disposition du gouvernement. Mention doit être portée sur cette décision qu'elle est devenue définitive.
4. Une décision des autorités visées à l'article 14, i, du Code pénal ordonnant l'internement d'un délinquant d'habitude, mis à la disposition du gouvernement.
5. Un arrêté ministériel de révocation de libération conditionnelle.
6. Un procès-verbal d'arrestation d'un condamné ou d'un interné évadé, lorsque le jugement ou l'arrêt de condamnation est coulé en force de chose jugée ou lorsque la décision d'internement est devenue définitive.
7. Une contrainte délivrée par l'autorité compétente en exécution des articles 159 et suivants de l'annexe 1 à la loi du 10 juillet 1963 portant les dispositions relatives à l'impôt sur les revenus.
8. Une décision de transfert prise par le gardien de la maison d'arrêt en exécution de l'article 35.

À la réception de tout prisonnier, il est procédé sur-le-champ à son inscription au registre d'écrou.

2.2.9 Répartition des détenus dans les locaux de détention

Les détenus sont en règle générale, enfermés dans les locaux, destinés à l'emprisonnement en commun. Les femmes sont séparées des hommes. Les mineurs âgés de moins de 18 ans ne seront incarcérés dans les prisons que s'il n'existe pas dans le ressort du tribunal de première instance, d'établissement de garde et d'éducation de l'État. À défaut d'existence d'un pareil établissement, ils seront détenus dans un quartier spécial. Dans la mesure où les installations le permettent, le gardien répartit les détenus dans les différents locaux de manière à grouper séparément :

1. les détenus condamnés à une peine de servitude pénale ne dépassant pas deux mois ;
2. les détenus condamnés à une peine de servitude pénale supérieure à deux mois ;
3. les délinquants d'habitude mis à la disposition du gouvernement en application du § 6 de la section 1 du livre 1er du Code pénal ;
4. les personnes mises à la contrainte par corps.

Le gardien peut décider que tel détenu sera enfermé dans un des locaux affectés à l'emprisonnement individuel. En cas d'encombrement, il peut placer plusieurs détenus dans un même local.

2.2.10 Libération conditionnelle

La libération conditionnelle n'est accordée qu'aux condamnés qui ont fait preuve d'amendement. L'administration, pour apprécier si un condamné qui a fait preuve d'amendement peut être libéré conditionnellement, tient compte de ses antécédents, des causes de la condamnation qu'il a encourue, de ses dispositions morales et des moyens d'existence dont il disposera à sa sortie de prison et de la durée déjà passée en prison(1/4 de la peine).

2.2.11 Évasions au sein des prisons

Lorsqu'un détenu s'est évadé, le gardien prévient immédiatement le premier bourgmestre ou le chef de la circonscription administrative territoriale du lieu de la prison, ou de la maison d'arrêt

ou du camp de détention. Il prévient en même temps le commandant local de la gendarmerie. Ces autorités prescrivent toutes mesures utiles pour reprendre l'évadé. Il leur fournit tous renseignements utiles pour faciliter les recherches. Le gardien envoie en outre un avis d'évasion au bureau central de signalement ainsi qu'à l'autorité judiciaire qui a prescrit l'incarcération s'il s'agit d'un prévenu. La matière de cette section est largement inspirée de l'ordonnance organique de 1964. Elle nous a présenté l'organisation du système pénitentiaire congolais.

2.3 Quelques anomalies du Système pénitentiaire Congolais

Il existe plusieurs dysfonctionnements dans le SPC. Mais nous avions pu relever dans cette section quelques dysfonctionnements en rapport avec la présente étude.

2.3.1 Anomalie liée à l'accès aux données

Un des dysfonctionnements dans le SPC est le manque de communication entre la capitale et les juridictions en provinces. Le journal officiel n'arrive que tardivement à l'intérieur du pays. C'est ainsi, par exemple, que les décrets présidentiels sur la grâce, l'amnistie ou la réduction de peine sont appliqués avec beaucoup de retard en faveur des prisonniers en provinces. Il faut aussi signaler que la non publication des jugements rendus par les juridictions dans les registres du Journal Officiel crée parfois de grandes disparités quant aux peines prononcées pour des infractions identiques. Il est à souligner que la difficulté d'accéder aux données de toutes les prisons occasionne un plus grand flou quant à chiffre exact de la population carcérale congolaise. Seulement, le dernier rapport portant sur les statistiques des détenus date de 2015.

2.3.2 Anomalie liée aux contrôles réguliers

En vue de surveiller la stricte observation des lois et règlements concernés, les lieux de détention doivent pouvoir être visités régulièrement par des personnes qualifiées et expérimentées. L'ordonnance numéro 344 du 17 septembre 1965 règle toutes les questions de contrôle des prisons par différentes personnes (inspecteur des établissements pénitentiaires, gouverneur ou son délégué, chef de la circonscription administrative territoriale, etc.) qui sont amenées à visiter régulièrement les lieux de détention.Ils doivent vérifier les registres d'écrou, le registre d'hébergement et s'assurer qu'aucun détenu n'est retenu au-delà du temps nécessaire pour être conduit devant l'autorité judiciaire compétente. En outre, ils contrôlent la tenue du dossier personnel du détenu. Malheureusement la plupart de ces contrôles ne fonctionnent plus. Le support papier utilisé ne leur facilite pas la tâche pour chercher les informations sur les prisonniers.

2.3.3 Anomalie liée au personnel

Le personnel pénitentiaire ou ce qu'il y a de personnel pénitentiaire n'est ni formé, ni rémunéré ni en nombre suffisant. Les quelques-uns du personnel que l'on trouve en poste sont d'un âge très avancé et ne sont plus aptes pour la plupart à exercer en tant que fonctionnaire de l'État. Dans d'autres prisons même, l'administration journalière est laissée à une auto gestion des détenus entre eux. De fois, ce sont des cahiers d'écoliers qui sont utilisés pour enregistrer les informations sur les détenus. Quelques unes possèdent des registres telle que prévue par l'ordonnance 344. D'autres prisons n'ont rien[2]. Eu égard à cela, l'application de certaines procédures administratives ne sont plus appliquées ou appliquées moyennant de l'argent.

2.3.4 Anomalie liée à la répartition des détenus dans les cellules

Le personnel pénitentiaire ne veille pas à une répartition rationnelle de l'espace disponible. D'où, on retrouve certaines cellules anormalement peuplées que d'autres et sans pourtant respectées ni la séparation entre la catégorie des détenus, ni l'âge, ni le type d'infraction commise, telles que stipulés dans l'ordonnance 344[1].

2.3.5 Anomalie liée à la durée de détention des détenus

Le manque de contrôle régulier par l'inspecteur et d'un personnel qualifié, occasionne une violation sur la durée de détention des prévenus. En effet, la durée de :
- la garde à vue est de 48 heure ;
- la détention préventive est de 60 jours[6] ;

Pourtant de nombreuses personnes sont arrêtées et ne sont souvent traduites devant les tribunaux qu'après des mois voire des années. Selon [6] par exemple, en novembre 2002, au Centre Pénitentiaire et de Rééducation de Kinshasa (CPRK), « 80% des personnes détenues sont poursuivies ou condamnées par la justice militaire. Sur ce pourcentage seul 10% des personnes sont condamnés et les autres 70% des personnes sont en majorité en détention préventive de plus de 12 mois ».

2.3.6 Anomalie liée à l'utilisation de la liberté conditionnelle

La libération conditionnelle des condamnés existe en droit congolais mais elle est très fortement sous-utilisée. Pour quelles raisons ? Certains gardiens en ignorent l'existence, d'autres ne la mettent pas en œuvre faute de moyens (formulaires, papier, etc.). Enfin, les lenteurs au sommet de la machine judiciaire et pénitentiaire finissent par en décourager plus d'un. Cela prive les détenus de la possibilité de demander le respect de leurs droits et de l'application de la procédure de libération conditionnelle dont un grand nombre de condamnés remplissent pourtant les conditions pour être bénéficiaires (ce qui contribuerait par ailleurs à une forte diminution de la surpopulation pénitentiaire).

2.4 Modélisation Métier

La modélisation du métier vise à mieux connaître le fonctionnement et les règles qui régissent le système organisationnel dans lequel on envisage implanter un nouveau système informatisé. Si l'on souhaite que le système informatique à concevoir corresponde aux exigences réelles du métier ciblé, il est vital de bien identifier les objectifs, les priorités, les règles de gestion et les processus clés de l'organisation avant toute tentative d'informatisation.

2.4.1 Structure organisationnelle d'une prison

Chaque prison est gardée et administrée par un gardien communément appelé Directeur de la prison, ayant le rang de chef de bureau et désigné par le ministre de la justice ou par son délégué parmi le personnel du cadre des services pénitentiaires. Il est chargé de :
- régler les détails de service de la prison ;
- assurer la garde des détenus et le maintien de l'ordre et de la discipline ;

– tenir les diverses écritures dans les registres ;
– assurer la conservation des biens des détenus ;
– assurer la conservation des documents et registres ;
– assurer la conservation des vivres,fournitures et matériels ;
Chaque directeur peut être secondé par un ou plusieurs greffiers pour la réalisation de ces différentes tâches. En cas de besoin, il peut avoir aussi un secrétaire. La surveillance immédiate des détenus est exercée par les surveillants ou à défaut par un corps de policiers. L'éducation des détenus est assurée par les instructeurs, chacun dans son domaine. Du point de vu administratif, la prison est gérée par le ministère de la justice.

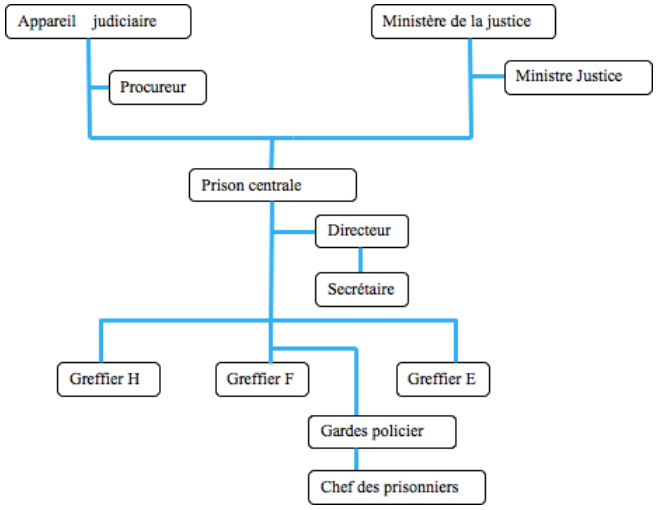


FIGURE 2.2 – organigramme du SPC

2.4.2 Missions du service pénitentiaire

Les missions du système pénitentiaire peuvent se résumer en ces termes :
– Enregistrement des informations sur des détenus dans des registres ;
– Organisation de l'encellulement des détenus ;
– Passation d'écriture dans des registres ;
– Gestion des visites ;
– Planification des sorties éventuelles à x échéance pour ceux dont la peine touche à sa fin ;
– Libération avec expiration des peines ;
– Notification des cas d'irrégularité en rapport avec la procédure pénale ;
– Gestion des transferts ;
– Recherche d'informations sur des détenus répondant à un profil donné ;
– Cotation des conduites ;
– Élaboration des rapports journaliers ;

2.4.3 Diagramme de flux d'information général

Le DFI est une représentation graphique d'un système d'information (SI) , qui identifie la manière dont les informations sont échangées (les flux), transformées (les traitements), et conservées (les dépôts d'information) en identifiant les entités externes qui sont les émetteurs (sources) et/ou les destinataires (destinations) de ces informations. La figure 2.2 et le tableau 2.1 donnent des détails sur le diagramme de flux d'information d'une prison.

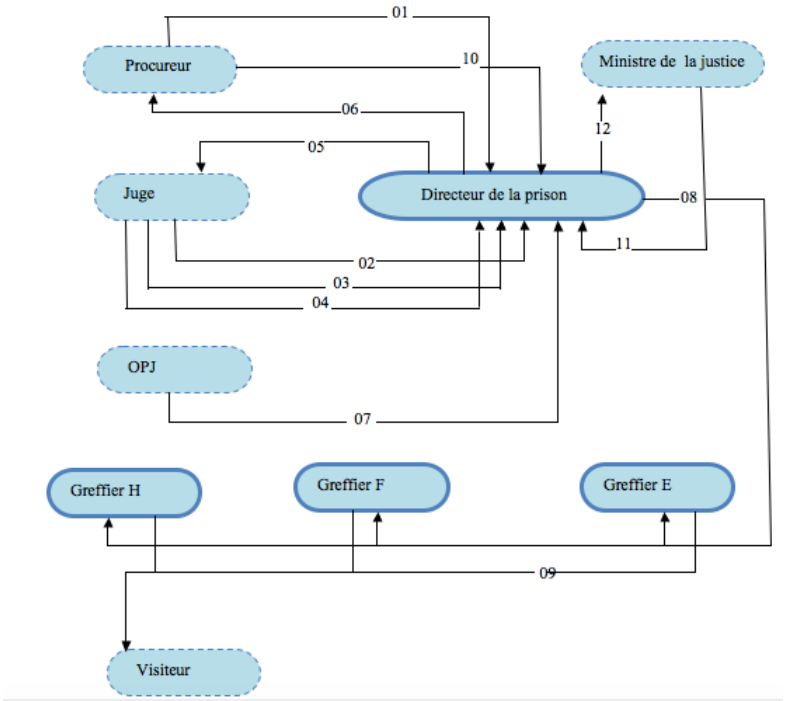


FIGURE 2.3 – organigramme du SPC

2.4.4 Étude des postes

Le poste de travail est une unité de l'organisation chargée d'un ensemble de tâches qui lui sont assignées afin de veiller à leur bonne exécution. L'objectif de cette phase est de recenser des postes de travail du système qui sera mis en place.C'est aussi une étape préalable pour l'identification des cas d'utilisation du futur système. Le tableau 2.2 renseigne sur les postes de travail du système pénitentiaire au sein d'une prison.

2.5 Analyse des procédures de travail

. Une procédure du travail est un ensemble de tâches qui concourent vers l'aboutissement d'un résultat prédéfini. L'objectif de cette section est de recenser toutes les procédures du travail. Nous pouvons citer quelques cas d'utilisations suivants :

- Écrou : il s'agit d'une opération qui consiste à saisir l'identité complète dans le registre d'écrou du détenu à incarcérer ainsi que d'autres détails sur l'infraction commise. Pendant cette procédure, le détenu doit choisir selon ses moyens financiers, le type des cellules où il doit être interné. S'il n'a pas fait de choix préalable, il devra être mis dans une cellule qui soit la moins peuplée. En plus, si c'est un récidiviste, il doit être mis dans une cellule spéciale. Dans ce cas, une sous procédure est importante pour détecter ce cas.
- Jugement : Cette opération consiste à effectuer un calcul de la date de sortie au cas où le détenu aurait été condamné. Mais elle consisterait aussi à libérer le détenu s'il était acquitté. Dans ce cas, on doit effectuer une sortie en le supprimant du registre d'écrou et en l'insérant dans le registre de sortant.
- Sortie : Cette opération consiste à effectuer une sortie du détenu de la prison. Il doit être supprimé du registre d'écrou et être mis dans le registre de sortant. Au cours de cette procédure, un billet de sortie signé par le directeur de la prison lui sera remis.

Table 2.2 – Flux d'information

Numéro	Désignation	Rôle
01	Mandat d'arrêt provisoire de l'officier du ministère Public	regroupe les informations sur l'inculpé ainsi que l'infraction
02	Ordonnance de détention préventive	regroupe toutes les informations identitaires du prévenu ainsi sur l'infraction commise
03	Ordonnance de confirmation de détention préventive	regroupe toutes les informations sur le prévenu
04	Ordonnance de confirmation de détention préventive renouvelée	regroupe toutes les informations sur le prévenu
05	Coupon juridictionnel	regroupe la liste de tous les détenus par juridiction
06	Rapport sur la population pénitentiaire	liste les statistiques des prisonniers par catégorie
07	Procès verbal de saisie des prévenus	regroupe toutes les informations identitaires du prévenu ainsi quel'infraction
08	Document01,02,03,04 pour enregistrement dans les registres	
09	Document fournissant l'information recherchée par un visiteur	
10	Réquisition aux fins d'emprisonnement	regroupe toutes les informations sur le prévenu
11	Demande d'information concernant les prisonniers	
12	Résultats de la requête soumise(listes des prisonniers par exemple)	

- Signalisation automatique : Cette procédure devra être une procédure automatique qui s'exécutera au démarrage du système. Il permettra de rechercher parmi les détenus ceux qui sont à leur expiration de peine au lieu que le greffier se met à le faire manuellement et péniblement dans le registre, d'une part. D'autre part il devra signaler tous les autres cas d'irrégularité.
- Rapports : Cette tâche consiste à élaborer des statistiques sur la population pénitentiaire par le directeur de la prison et à soumettre à sa hiérarchie.
- Recherche : Cette opération consistera à saisir les critères de recherches et une liste des prisonniers s'affiche automatiquement ;
- Visite : Cette tâche vise à fournir toutes les informations utiles aux personnes visiteurs concernant un prisonnier donné. Signalons que lorsqu'un prisonnier est sanctionné par le fait de ne pas être visité pendant une certaine période,il ne lui sera pas permis d'entrer en contact avec la personne qui vient lui rendre visite.
- Hospitalisation : Cette tâche consiste à compléter les informations dans le dossier médical du

Table 2.3 – Description des postes de travail

Désignation	Structure de rattachement	Responsabilité du poste
Ministère de la justice	Ministère de la justice	– Mettre en place des politiques d'amnistie,grâce,etc ; – Uniformiser la durée de peine par infraction ;
Inspecteur des établissements pénitentiaires	Ministère de la justice	– Contrôler les différents registres de la prison ; – Signaler une situation irrégulière ;
Directeur de la prison	Prison	– Réceptionner un prisonnier ; – Établir la synthèse de l'activité journalière ; – Contrôler périodiquement l'activité des greffiers ; – Assurer la relation avec la haute hiérarchie ainsi que les partenaires externes ;
Greffier	Prison	– Enregistrer les informations des détenus dans le registre d'écrou ; – Calculer la date de sortie en cas de condamnation ; – Repartir les détenus dans les cellules ; – Passer des écritures dans les différents registres lors de l'hospitalisation,sortie,évasion,etc ; – Réceptionner les visiteurs pour leur fournir d'indication sur les prisonniers ;
Secrétaire	Prison	– Communication interne et externe ; – Conserver des documents administratifs ;
Acteur extérieur(Police,avocat,etc)	Monde Extérieur	Rechercher des informations sur les prisonniers ;

détenu.

2.6 Conclusion au chapitre d'analyse de l'existant

Après avoir fait le constat du problème au premier chapitre, il est important de l'étudier en détail en vue de le résoudre. En général, pour résoudre un problème, il faut d'abord bien le poser ou le formaliser. Cette étape nécessite à son tour, une analyse du problème dans le but de dégager les caractéristiques essentielles de ce dernier. Voilà pourquoi nous avions, dans ce chapitre, analyser le SPC du point de vue flux d'information, postes de travail et ses missions.

Chapitre 3

CONCEPTION DU NOUVEAU SYSTÈME A L'AIDE D'UML

3.1 Présentation du langage UML

3.1.1 Introduction

Le langage UML(Unified Modeling Langage) est un langage de modélisation qui a pour but de faciliter les transitions, lors du développement d'un projet informatique, du besoin originel à la phase d'implémentation[8]. Ce langage, fusion de 3 méthodes orientées objet très utilisées(OMT(Object modeling Technique),Booch et OOSE(Object Oriented Software Enginee ring)) dont le développement a débuté en 1994, et qui a été standardisé en 1997 par l'OMG(Object Management Group) dans sa version 1.1, s'appuie essentiellement sur la technologie objet et les concepts qu'elle véhicule.

En tant que langage de modélisation, l'UML couvre un spectre plus large que les bases de données. Son utilisation peut servir au développement des systèmes informatisés de gestion, de temps réel, de l'embarqué tout comme à la résolution des problèmes d'organisation de tout style. De plus, UML, de part sa représentation essentiellement graphique, se veut extrêmement vulgarisé et intuitif, et est utilisé par les êtres humains ainsi que les machines[10].

On parle volontairement de langage UML et non pas de méthode, car UML propose des outils et des concepts de modélisation, et non pas une méthodologie à respecter scrupuleusement. C'est pourquoi, dans ce présent travail, nous allons utiliser seulement 3 diagrammes à savoir le diagramme de cas d'utilisation, le diagramme de classe et le diagramme de déploiement. Le diagramme de cas d'utilisation nous permettra de concevoir l'interface de l'application. Le diagramme de classe, lui, interviendra pour la conception de la structure de la base des données et enfin un diagramme de déploiement pour concevoir l'architecture physique de la mise en œuvre du système pour utilisation. Dans les lignes qui suivent, nous présentons rapidement les 13 diagrammes d'UML.

3.1.2 Diagrammes d'UML

La modélisation proposée par le langage UML se réalise principalement sous forme graphique, en usant de divers types de diagrammes spécifiques, repartis en deux groupes :

- structure du système(statique)
  - diagramme de cas d'utilisation :structure des fonctionnalités ;
  - diagramme de classes :structure des entités ;
  - diagrammes d'objets :cas particuliers des structures de classes ;
  - diagramme de composants :structure de l'architecture logicielle ;
  - diagramme de déploiement :structure de l'architecture matérielle ;
  - diagramme de packages
  - diagramme de structure composite
- comportement du système(dynamique)
  - diagrammes d'états-transitions : cycle de vie des objets ;
  - diagrammes d'activités ;
  - interaction du système :
    - diagrammes de séquence : scénarios des fonctionnalités
    - diagrammes de collaboration/communication :interaction entre objets ;
    - diagramme de vue globale des interactions
    - diagrammes de temps

3.2 Modélisation du système

Dans cette section nous présenterons 3 diagrammes à savoir le diagramme de cas d'utilisation, le diagramme de classe et le diagramme de déploiement du nouveau système conçu.

3.2.1 Diagramme de cas d'utilisation

Définition 3.1 *Le diagramme de cas d'utilisation sert à schématiser l'expression des besoins. L'ensemble des schémas constitue une base de travail pour construire les interfaces graphiques du système.*

Il se présente sous 2 formes :
- schéma regroupant les activités d'un acteur(vision du système par l'acteur) ;
- tableau détaillant les actions liées à une activité.

Syntaxe

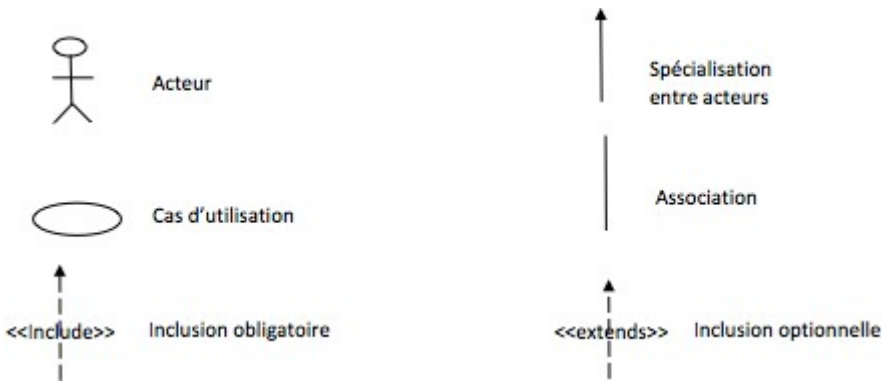


FIGURE 3.1 – symboles utilisés dans la construction des cas d'utilisations

Description sémantique des symboles Un acteur est une entité extérieure au système modélisé et qui interagit directement avec lui. Un cas d'utilisation est un service rendu à l'utilisateur, il implique des séries d'actions plus élémentaires. Les acteurs impliqués dans un cas d'utilisation lui sont liés par une association. La relation "include" implique une action obligatoire à réaliser avant l'exécution du cas concerné. La relation "exclude" implique une action optionnelle à réaliser par rapport à un cas concerné.

3.2.2 Identification des Diagramme de cas d'utilisation du système conçu

Nous allons regrouper les cas d'utilisations dans un diagramme par acteur de notre système.
– Acteur :Greffier

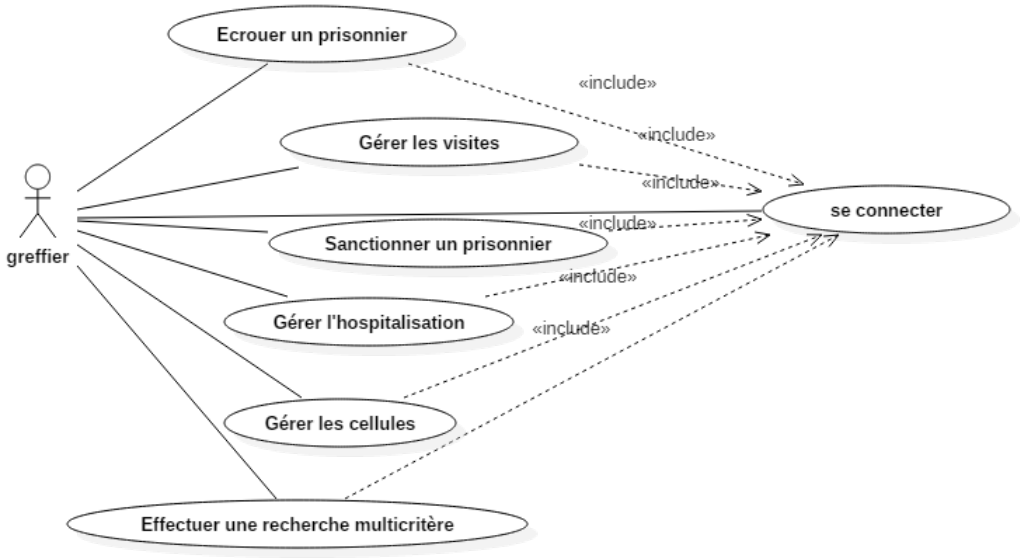


FIGURE 3.2 – Cas d'utilisation «Effectuer les opérations pénitentiaires»

Nous devrons détailler par la suite chaque d'utilisation dans un tableau. Pour ce faire, nous l'avions fait pour quelques cas complexes et principaux par rapport à cet acteur.

Table 3.1 – Cas d'utilisation «se connecter»

cas d'utilisation	se connecter
Acteur	greffier
Ev.déclencheur	néant
Intérêts	Accéder au serveur afin d'être authentifié et accéder à l'application.
Pré-conditions	serveur actif
Post-condition	Connexion établie
Scenario nominal	1. L'utilisateur saisit son user-name et mot de pass ; 2. L'utilisateur demande une connexion en cliquant sur bouton valider ; 3. Le serveur répond.

Table 3.2 – Cas d'utilisation «Écrouer un prisonnier»

cas d'utilisation	Ecrouer un prisonnier
Acteur	greffier
Ev.déclencheur	néant
Intérêts	Enregistrer les informations du détenu dans la base des données.
Pré-conditions	authentification réussie
Post-condition	Les informations du détenu sont enregistrées
Scenario nominal	1. L'utilisateur saisit toutes les informations relatives au détenu ; 2. L'utilisateur demande au système une chambre disponible par rapport à la catégorie choisie ; 3. L'utilisateur demande l'enregistrement des données par le clic sur valider. 4. Le système répond.
Contraintes	l'un des champs obligatoire n'est pas rempli,aller à 1

Table 3.3 – Cas d'utilisation «Gérer l'hospitalisation»

cas d'utilisation	Gérer l'hospitalisation
Acteur	greffier
Ev.déclencheur	néant
Intérêts	Garder la trace de l'état de santé de chaque détenu.
Pré-conditions	authentification réussie
Post-condition	enregistrement des informations sur l'état de santé des détenus
Scenario nominal	1. L'utilisateur choisit le prisonnier ; 2. L'utilisateur précise les détails sur la maladie ; 3. L'utilisateur valide l'opération. 4. Le système répond.
Contraintes	l'un des champs obligatoire n'est pas rempli,aller à 1

Table 3.4 – Cas d'utilisation «Effectuer une recherche multi-critère»

cas d'utilisation	Effectuer une recherche multi-critère
Acteur	greffier
Ev.déclencheur	néant
Intérêts	Obtenir les informations recherchées sur base de plusieurs critères.
Pré-conditions	authentification réussie
Post-condition	Affichage des informations respectant les critères
Scenario nominal	1. L'utilisateur précise les critères de recherche 2. L'utilisateur valide l'opération ; 3. L'utilisateur valide l'opération. 4. Le système répond.
Contraintes	l'un des champs obligatoire n'est pas rempli,aller à 1

– Acteur :Directeur de la prison

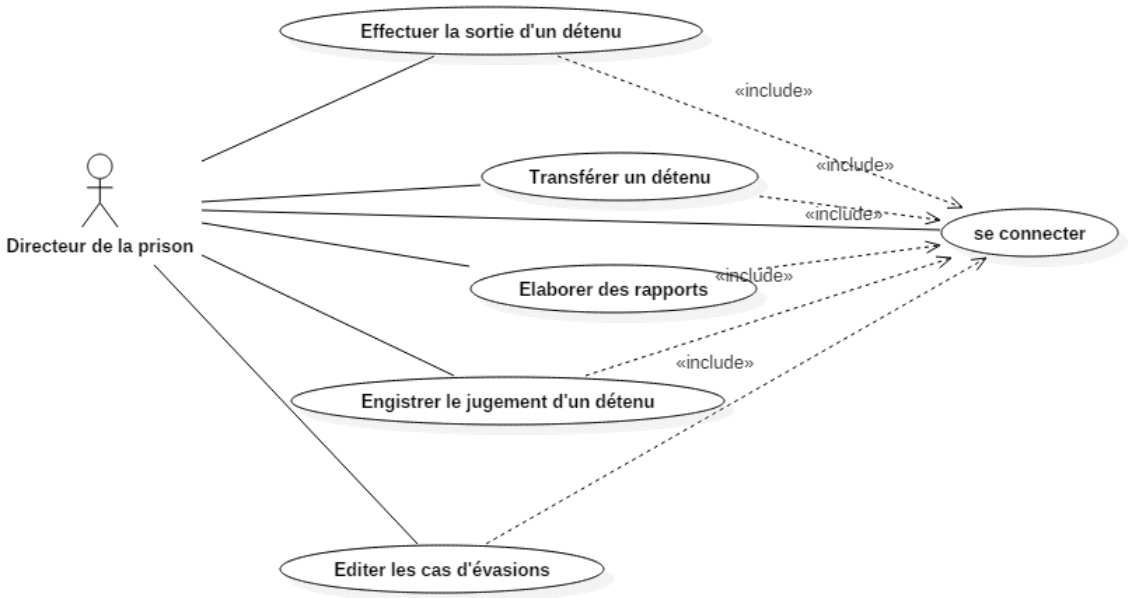


Figure 3.3 – Cas d'utilisation «Gérer le dossier administratif du détenu»

Table 3.5 – Cas d'utilisation «Effectuer la sortie d'un détenu»

cas d'utilisation	Effectuer la sortie d'un détenu
Acteur	Directeur de la prison
Ev.déclencheur	néant
Intérêts	Libérer un prisonnier de la prison.
Pré-conditions	authentification réussie
Post-condition	Sortie du détenu
Scenario nominal	1. L'utilisateur choisit le prisonnier à libérer, saisit le motif de libération ; 2. L'utilisateur valide l'opération ; 3. Le système imprime automatiquement un billet de sortie.
Contraintes	l'id du détenu n'est pas choisi,aller à 1

Table 3.6 – Cas d'utilisation «Élaboration des rapports»

cas d'utilisation	Élaboration de rapports
Acteur	Directeur de la prison
Ev.déclencheur	néant
Intérêts	Impression automatique de rapports.
Pré-conditions	authentification réussie
Post-condition	impression des rapports
Scenario nominal	1. L'utilisateur choisit le type de rapports, ; 2. L'utilisateur valide l'opération ; 3. Le système imprime automatiquement le rapport choisi
Contraintes	le rapport n'est pas choisi ,aller à 1

– Acteur :Ministère de la justice

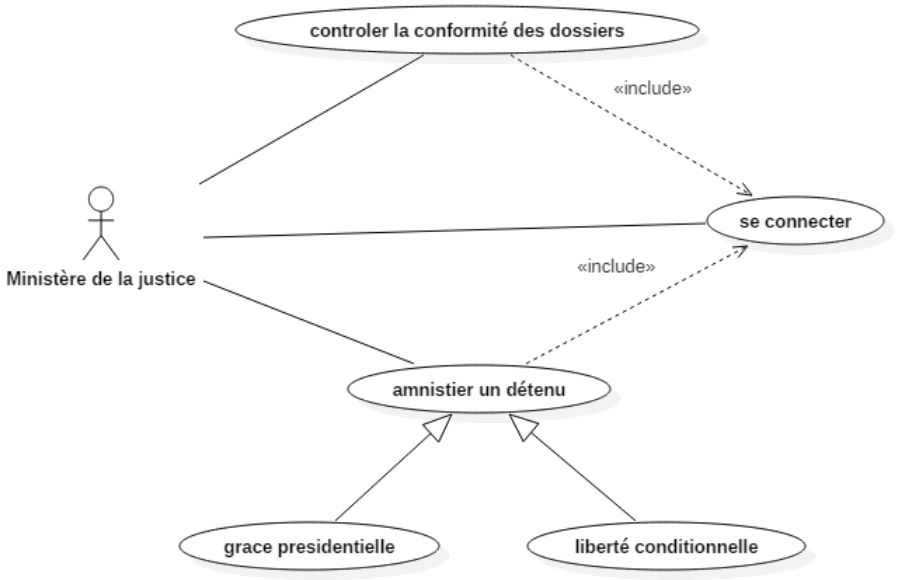


FIGURE 3.4 – Ministère de la justice

TABLE 3.7 – Cas d'utilisation «Amnistier un détenu»

cas d'utilisation	Amnistier un détenu
Acteur	Ministère de la justice
Ev.déclencheur	néant
Intérêts	Libération conditionnelle d'un détenu.
Pré-conditions	authentification réussie
Post-condition	Libération conditionnelle d'un détenu.
Scenario nominal	1. L'utilisateur peut choisir la libération conditionnelle ; 2. L'utilisateur peut soit choisir une politique de grâce ;
Contraintes	Rien

– Acteur :Avocat-Police

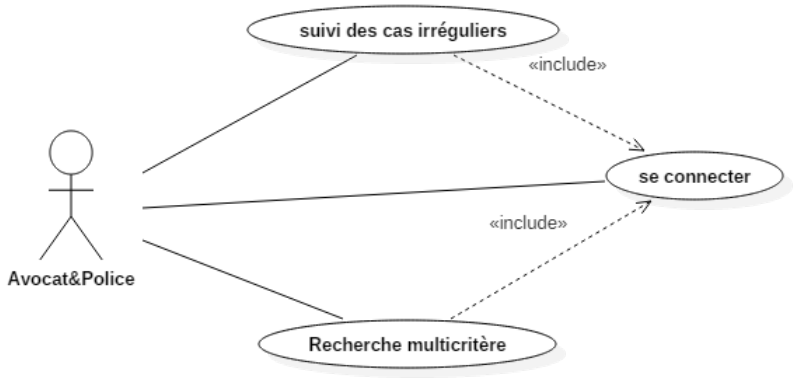


FIGURE 3.5 – Cas d'utilisation «Recherche information»

TABLE 3.8 – Cas d'utilisation «suivi des cas irréguliers»

cas d'utilisation	Suivi des cas irréguliers
Acteur	Avocat-Police
Ev.déclencheur	néant
Intérêts	Retrouver tous les cas irréguliers.
Pré-conditions	authentification réussie
Post-condition	Affichage des cas irréguliers.
Scenario nominal	1. L'utilisateur choisit une durée expirée ; 2. L'utilisateur valide l'opération ;
Contraintes	Rien

3.2.3 Diagramme des classes

Définition 3.2 *Le diagramme de classes représente, de manière statique, les classes qui composent le système, ainsi que les relations entre elles[16].*

Le but est de décrire :
– la structure interne précise de chacune des classes(attributs et méthodes) ;
– les relations entre les classes mis en œuvre
Pour la modélisation des bases de données, les méthodes sont surtout utilisées pour représenter des données calculées (à l'instar des attributs dérivées) ou pour mettre en exergue des fonctions importantes du système cible. Seules les méthodes les plus importantes sont représentées, l'approche est moins systématique qu'en modélisation objet par exemple.[9] Syntaxe

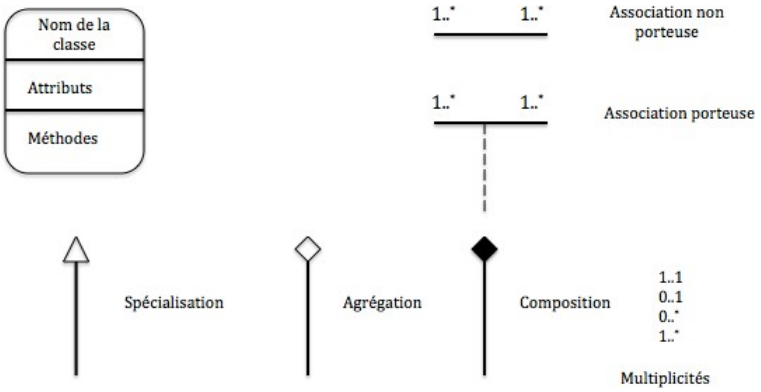


FIGURE 3.6 – symboles utilisés dans la construction du diagramme des classes

Description sémantique des symboles utilisés La définition d'une classe comprend les éléments suivants :
- nom de la classe : Description du modèle d'objet ;
- attributs : informations qualifiant l'objet ;
- méthodes : opérations, actions et réaction de l'objet, fonctions associées à la classe.

Une association est une relation structurelle entre objets. Elle est souvent utilisée pour représenter les liens possibles entre objets de classes données. La notion de multiplicité permet le contrôle du nombre d'objets intervenant dans chaque instance d'une association. Une agrégation est une forme particulière d'association. Elle représente la relation d'inclusion d'un élément dans un ensemble. La relation de composition décrit une contenance structurelle entre instances. Il s'agit d'une agrégation forte. La relation de spécialisation permet à la classe spécialisée d'hériter la structure et le comportement de la classe mère.

3.2.4 Construction du diagramme de classe

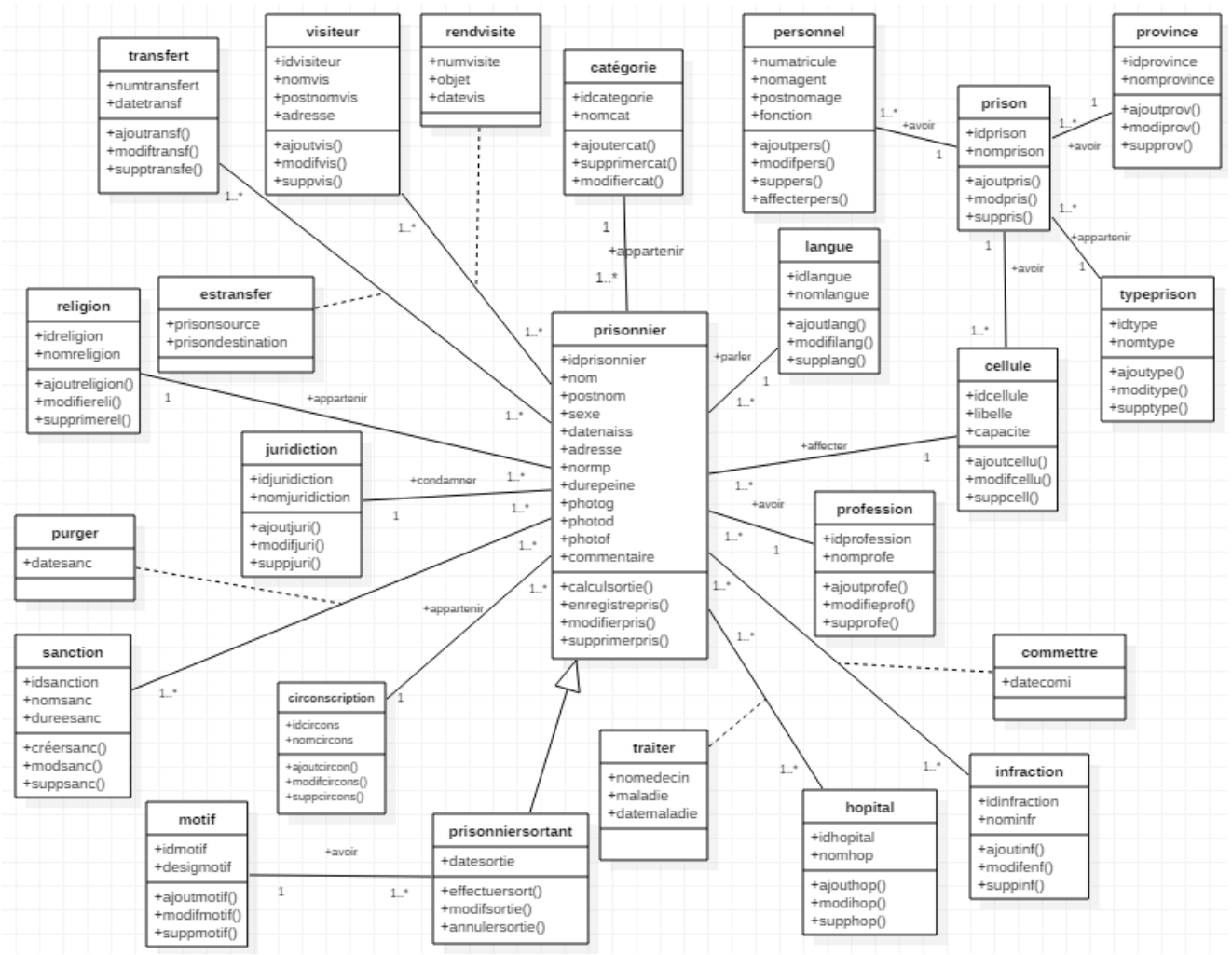


FIGURE 3.7 – Diagramme des classes

Pour concevoir nos requêtes en algèbre relationnelle, il est important d'avoir le modèle logique des données de notre système.

3.3 Modèle Logique des données du nouveau système

Définition 3.3 *Le modèle logique des données permet de modéliser la structure selon laquelle les données seront stockées dans la future base des données.*

Notre base de données sera réalisée suivant le principe de l'algèbre relationnelle.

3.3.1 Règles de passage du diagramme de classes au modèle logique

Pour traduire le diagramme des classes vers le modèle logique relationnel, on peut appliquer les règles suivantes :

- Chaque classe donne naissance à une relation. Chaque attribut de cette classe devient un attribut de la relation. L'identifiant est conservé en tant que clé de la relation.
- Chaque classe-association dont aucune patte n'a pour multiplicité maximale 1 donne naissance à une relation. Chaque attribut de cette classe-association devient un attribut de la relation. L'identifiant, s'il est précisé, est conservé en tant que clé de la relation, sinon cette clé est formée par la concaténation des identifiants des classes qui interviennent dans la classe-association.
- Une classe-association dont au moins une patte a une multiplicité maximale à 1 (cette classe-association devrait être binaire et n'a généralement pas d'attribut) ne devient pas une relation. Il décrit en effet une dépendance fonctionnelle. La relation correspondant à la classe dont la patte vers la classe-association a une multiplicité maximale valant 1, se voit simplement ajouter comme attribut (et donc comme clé étrangère) l'identifiant de l'autre classe.

3.3.2 Élaboration du modèle logique

En appliquant les différentes règles émises ci-dessus sur le diagramme de classe à la figure suivante. on obtient les relations suivantes :

- prisonnier(idprisonnier, #idcategorie, #idreligion, #idjuridiction, #idcircons, #idprofession, #idlangue, #idcellule, nom, postnom, sexe, datenaiss, adresse, normp, durepeine, photog,photod, photof,commentaire)
- categorie(idcategorie, nomcategorie)
- religion(idreligion, nomreligion)
- juridiction(idjuridiction, nomjurid)
- circonscription(idcircons, nomcircons)
- profession(idprofession, nomprofe)
- cellule(idcellule, #idprison, libelle,capacite)
- prison(idprison, #idtype, #idprovince, nomprison)
- personnel(numatricule, #idprison, nomagent, postnomagent, fonction)
- typeprison(idtype, nomtype)
- province(idprovince, nomprov)
- infraction(idinfraction, nominfr)
- commettre(idprisonnier, idinfraction, datecomi)
- visiteur(idvisiteur, nomvis, postnomvis, adresse)
- rendvisite(numvisite, #idprisonnier, #idvisiteur, objet, datevis)
- sanction(idsanction, nomsanc, dureesanc)
- purger(idprisonnier, idsanction, datasanc)
- motif (idmotif , designamoti)
- prisonniersortant(idprisonnier, datesortie)
- hopital(idhopital, nomhopital)
- traiter(idprisonnier, idhopital, nomedecin, maladie, datemaladie)
- transfert(inumtransfert, datetransf)
- estransfer(idprisonnier, numtransfert, prisonsource, prisondestination)
- users(iduser, nomuser, motpass)

3.3.3 Diagrammes de déploiement

Définition 3.4 *Le diagramme de déploiement représente l'organisation physique de la distribution des composants logiciels de l'application.*

Ce diagramme fait parti des diagrammes structuraux(statiques) Il est ainsi composé :
- des ressources matérielles qui constituent le système et montre la répartition des composants (élément logiciels) sur ces matériels ;
- des liens de communication entre les différentes ressources matérielles.

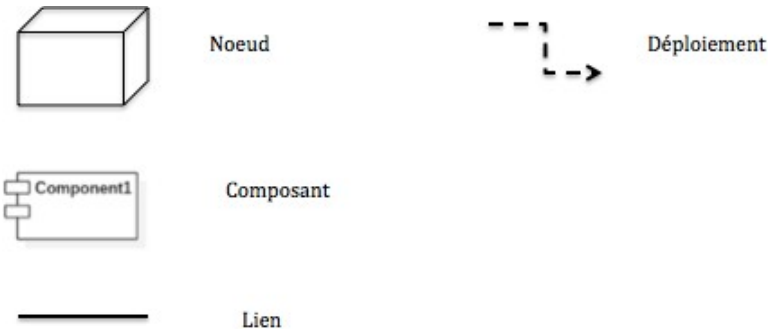


FIGURE 3.8 – symboles utilisés dans la construction du diagramme de déploiement

Description sémantique des symboles utilisés Un nœud représente une ressource matérielle du système. En général, cette ressource possède au minimum de la mémoire et parfois aussi des capacités de calcul. Un composant réside dans le nœud. Il représente un élément logiciel. Il peut être soit placé dans le nœud soit relié par une relation de dépendance(déploiement) au nœud. Un lien représente les moyens de communication entre les nœuds. Signalons qu'il existe d'autres symboles mais que nous n'avions pas utilisés dans notre conception.

3.3.4 Construction du diagramme de déploiement

Comme on peut le constater sur la figure 3.9, chaque province aura besoin d'un serveur pour gérer les données locales. Nous pouvons avoir plusieurs machines clientes pour accéder aux données et à l'application du système pénitentiaire. Ensuite, tous les serveurs locaux seront en liaison avec le serveur central se trouvant en capital. Les données pourront être chaque fois répliquées au niveau central après les heures de service en province. Le serveur central peut à son tour, faire une copie de la base des données centrale sur chaque serveur local étant donné que le lien est bidirectionnel. Ceci permettra une disponibilité de toutes les données du système pénitentiaire congolais sur chaque serveur en province. C'est l'approche classique pour déployer une base des données reparties.[24][25]

La figure 3.10 présente une autre possibilité de déploiement d'une base des données reparties utilisant le modèle client serveur mais tout en essayant de reproduire les caractéristiques de l'approche classique. Comme nous pouvons le remarquer sur la Figure 3.10, nous avons un seul serveur qui héberge l'ensemble des applications et base des données de toutes les prisons, et les différentes prisons en province sont considérées comme des clients. Pour cette deuxième approche, une connexion internet s'impose pour l'utilisation de l'application en locale, ce qui n'était pas le cas pour la première approche. Lorsqu'une une prison se connecte à la base des données, un mécanisme de filtration des données est mise en place pour garantir l'utilisation des données locales spécifiques à la prison concernée. Concluons en disant que chaque approche a ses avantages et inconvénients.

Pour le cadre de cette étude, nous avions choisi d'utiliser la deuxième approche car elle était réalisable par rapport à nos moyens. Pour le premier modèle de déploiement, nous devrions

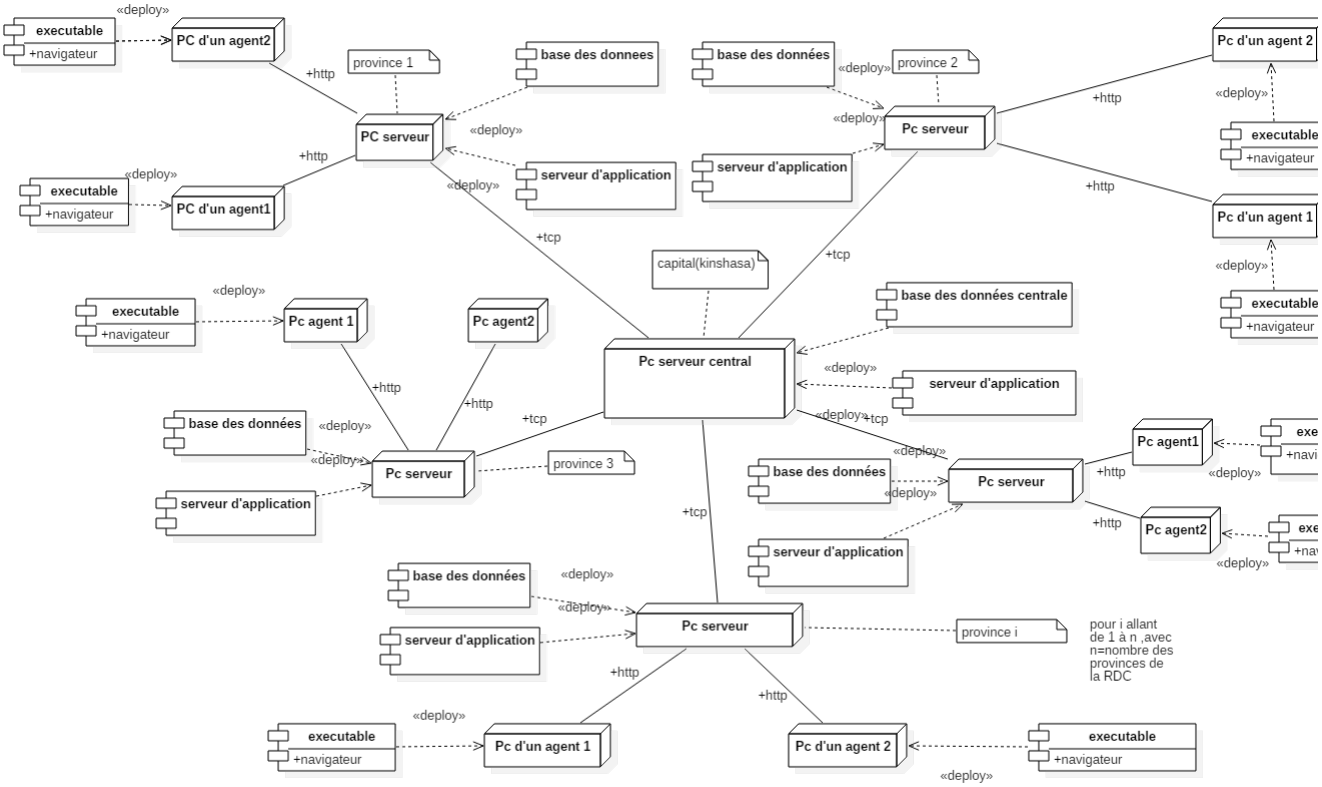


FIGURE 3.9 – Diagramme de déploiement en local

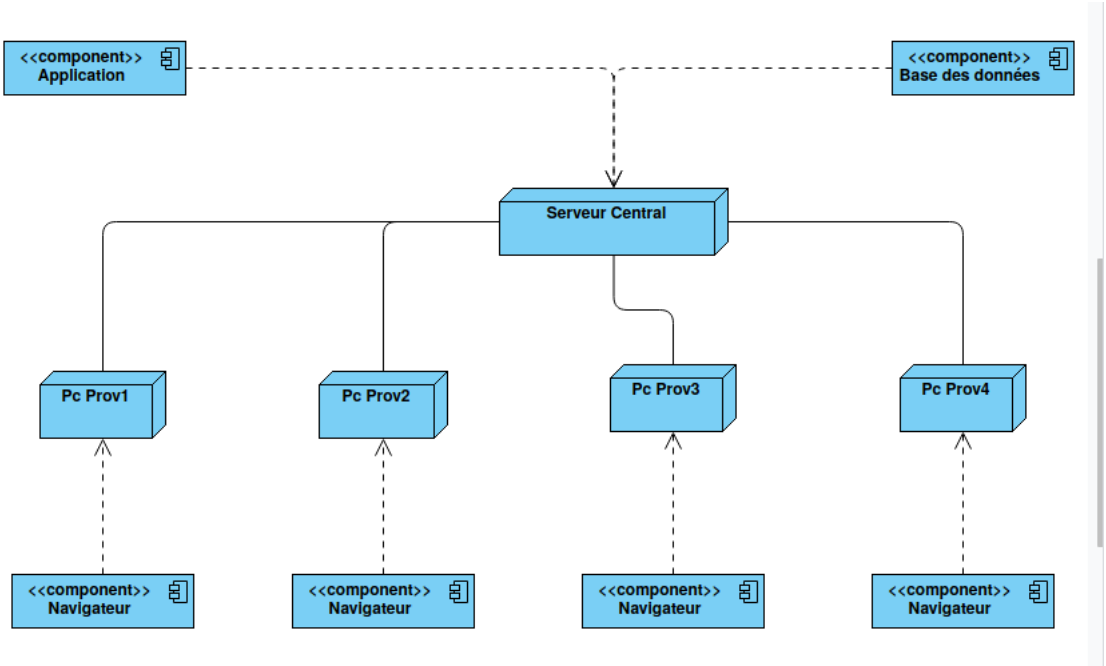


FIGURE 3.10 – Diagramme de déploiement en ligne

utiliser Oracle qui facilite la répartition des données mais ce dernier exige une licence pour la version dont l'application est accessible en ligne.

3.4 Conclusion au chapitre sur la conception du système

Avant qu'une maison n'existe, elle existe d'abord sur papier. Cela signifie que sa construction sera faite sur base de son image sur papier. Dans le cadre de construction du système d'information informatisé comme c'est bien notre cas, nous partageons aussi la même philosophie . Nous avions construit l'ossature de l'application informatique dans ce chapitre grâce aux différents diagrammes UML. Ces modèles construits, constituent des représentations des solutions au problème que nous cherchons à résoudre dans ce travail. La construction du système nécessitant en général, plus d'une personne, ces représentations sont aussi la base de communication entre différents acteurs intervenant. Nous avions réalisé le diagramme de cas d'utilisation, le diagramme de classes et enfin le diagramme de déploiement.

Chapitre 4

MODÈLE MATHÉMATIQUE UTILISE POUR LA RÉALISATION DES REQUÊTES

4.1 Introduction

Toutes les fonctionnalités du système se traduisent par une sorte des requêtes à construire. Dans ce chapitre nous allons présenter les opérateurs de l'algèbre relationnelle et montrer son importance dans la construction des requêtes SQL.

4.2 Modèle Relationnel

4.2.1 Définition, historique et évolution

Définition 4.1 *L'Algèbre Relationnelle a été inventée par E. Codd comme un ensemble d'opérateurs pour manipuler les relations ou tables d'une base des données relationnelle.[12]*

Nous pouvons faire un parallélisme avec l'arithmétique qui fournit les opérations de base pour manipuler les nombres(addition,soustraction, multiplication et division). Tout comme l'arithmétique, ces opérateurs d'algèbre relationnelle prennent en entrée des relations et produisent en sortie des relations ou tables.

L'algèbre relationnelle constitue le fondement théorique du langage standard SQL qui est utilisée pour localiser des données dans la base répondant à un critère. Notons tout de même une certaine nuance entre l'algèbre relationnelle et le SQL. Le SQL est un langage déclaratif qui permet de caractériser le résultat attendu sans dire comment l'obtenir. Par contre, l'algèbre relationnelle est un langage procédural qui permet de décrire l'enchaînement des opérateurs qui permettront d'obtenir un résultat.

C'est ainsi que tous les SGBD relationnels utilisent l'algèbre relationnelle pour trouver des plans d'exécution en vue d'optimiser les requêtes. En effet, pour une requête SQL donnée, il existe plusieurs requêtes algébriques équivalentes(ie plusieurs requêtes en algèbre relationnelles qui retournent les mêmes tuples ou résultats) obtenus en appliquant des règles de réécriture appelées aussi lois algébriques. Autant les tuples retournés sont les mêmes pour tous ces plans d'exécution, autant le temps nécessaire pour obtenir ces tuples, lui peut être différent. Tout dépend de la façon dont les opérations qui composent le plan d'exécution sont organisés.

4.2.2 Justification du choix de ce modèle

Nous avons choisis ce modèle mathématique pour qu'il nous aide à bien construire nos requêtes. Puisque plus une requête est trop complexe(ie plusieurs blocs select) plus le système a très peu de plans d'exécution. Par contre, le système a des degrés de liberté suffisants si la requête est à plat ie en un seul bloc. Par conséquent, nos tâches principales s'exécuteront dans un temps raisonnablement bon. La conception de nos requêtes en algèbre relationnelle nous permettra très facilement d'écrire des requêtes simples en SQL.

4.2.3 Opérateurs de l'algèbre relationnelle

Il existe deux grandes catégories d'opérateurs[13][26] :
- des opérateurs de base ;
  - Sélection ;
  - Projection ;
  - Union ;
  - Différence ;
  - Produit cartésien ;
  - Renommage.
- des opérateurs dérivés.
  - Intersection ;
  - Jointure ;
  - Division.

1. Sélection
   Soit $R(a_1, a_2, ...a_N)$une relation. La sélection travaille sur R et définit une relation qui ne contient que les tuples de R qui satisfont à la condition (ou prédicat) spécifiée. Elle est notée :

$$\sigma_{predicat}(R)$$

2. Projection
   Soit $R(a_1, a_2, ...a_N)$une relation. La projection travaille sur R et définit une relation restreinte à un sous-ensemble des attributs de R, en extrayant les valeurs des attributs spécifiés et en supprimant les doublons. Elle est notée :

$$\pi_{a_1, a_2, ...a_k}(R)$$

3. Union
   Soient $R(a_1, a_2, ...a_N)$et $S(b_1, b_2, ...b_M)$ deux relations. L'union de deux relations R et S définit une relation qui contient tous les tuples de R, de S ou à la fois de R et S, les tuples en double étant éliminés. Elle se note :

$$R \cup S$$

4. Différence
   Soient $R(a_1, a_2, ...a_N)$et $S(b_1, b_2, ...b_N)$ deux relations. La différence d'ensemble définit une relation qui comporte les tuples qui existent dans la relation R et non dans la relation S. Elle se note :

$$R - S$$

5. Produit cartésien
   Soient $R(a_1, a_2, ...a_N)$et $S(b_1, b_2, ...b_N)$ deux relations. Le produit cartésien définit une relation constituée de la concaténation de tous les tuples de la relation R avec tous ceux de la relation S. Elle se note :
   $$R \times S$$

6. Renommage
   Cet opérateur permet de changer le nom d'un ou plusieurs attributs d'une relation R. Elle se note :
   $$\propto [nomattribut : nouveaunom, ...]R$$

7. Intersection
   Soient $R(a_1, a_2, ...a_N)$et $S(b_1, b_2, ...b_N)$ deux relations. L'intersection définit une relation constituée de l'ensemble de tous les tuples présents à la fois dans R et dans S. Elle se note :
   $$R \cap S$$

8. Theta-Jointure
   La theta-jointure définit une relation qui contient les tuples qui satisfont le prédicat P du produit cartésien de R et S. Le prédicat P est de la forme $R.a_i \theta S.b_j$ où θ est l'un des opérateurs de comparaison(>,<,>=,<=). Lorsque l'opérateur de comparaison est (=) on parle d'équi-jointure. Elle se note :
   $$R \bowtie_P S$$

9. Jointure Naturelle
   La jointure naturelle est une équi-jointure des relations R et S sur tous les attributs communs en retirant les occurrences multiples d'attributs. Elle se note :
   $$R * S$$

10. Division
    Supposons que la relation R soit définie sur l'ensemble d'attributs A et que la relation S soit définie sur l'ensemble d'attributs B, de telle sorte que $B \subseteq A$. Soit $C = A - B$ La division définit une relation sur les attributs C, constituée de l'ensemble des tuples de R qui correspondent à la combinaison de tous les tuples de S. Elle se note :
    $$R \div S$$

4.2.4 Fonctions d'agrégat en Algèbre Relationnelle

Nous introduisons l'opérateur $a_1, ...a_n \gamma F_1(a_{n+1}, ...a_p), ...F_k(a_{n+1}, ...a_p)$pour l'algèbre relationnelle. Cet opérateur regroupe ensemble tous les n-uplets qui ont la même valeur sur les attributs $a_1, ...a_n$ puis calcule pour chacun de ces groupes la valeur des fonctions $F_1(a_{n+1}, ...a_p)$ $, ...F_k(a_{n+1}, ...a_p)$. Notons qu'implicitement une projection est effectuée sur les attributs $a_1, ...a_n$, auxquels on rajoute les valeurs des fonctions. Si on ne met aucun ensemble d'attributs, alors tous les n-uplets de la table sont regroupés ensembles. On peut également ne pas calculer aucune valeur de fonction. Dans ce cas, le GROUP BY revient à faire un DISTINCT dans le SELECT.

4.2.5 Règles de réécriture

Il s'agit d'un ensemble des propriétés qui permettent de transformer une expression algébrique en une autre équivalente.|[27]

- Commutativité des jointures

$$R \bowtie S \equiv S \bowtie R$$

- Associativité des jointures

$$(R \bowtie S) \bowtie T \equiv R \bowtie (S \bowtie T)$$

- Regroupement des sélections

$$\sigma_{A='a' \wedge B='b'}(R) \equiv \sigma_{A='a'}(\sigma_{B='b'}(R))$$

- Commutativité de la sélection et de la projection

$$\pi_{A_1,A_2,...,A_p}(\sigma_{A_i='a'}(R)) \equiv \sigma_{A_i='a'}(\pi_{A_1,A_2,...,A_p}(R), i \in 1,...p$$

- Commutativité de la sélection et de la jointure

$$\sigma_{A='a'}(R(...A...) \bowtie S) \equiv \sigma_{A='a'}(R) \bowtie S$$

- Distributivité de la sélection sur l'union

$$\sigma_{A='a'}(R \cup S) \equiv \sigma_{A='a'}(R) \cup \sigma_{A='a'}(S)$$

- Commutativité de la projection et de la jointure

$$\pi_{A_1,A_2,...,A_p}(R) \bowtie A_i = B_j \pi_{B_1,B_2,...,B_q}(S), i \in 1,...pj \in 1,...q$$

- Distributivité de la projection sur l'union

$$\pi_{A_1,A_2,...,A_p}(R \cup S) \equiv \pi_{A_1,A_2,...,A_p}(R) \cup \pi_{A_1,A_2,...,A_p}(S)$$

4.2.6 Conception de nos requêtes en Algèbre Relationnelle

Dans cette section, nous allons présenter quelques requêtes de base du fonctionnement de nouveau système en algèbre relationnelle. Nous allons nous appuyer sur les cas d'utilisations que nous avions conçus.

- Cas d'utilisation "se connecter" Dans ce cas d'utilisation l'utilisateur devra saisir son mot de pass et son nom d'utilisateur. Ensuite le système devra vérifier dans la base de donnée si ces données existent réellement. Pour accomplir cette tâche, il est important d'utiliser la requête suivante :

$$\sigma_{nomuser='nomsaisi' \wedge motpass='motdepasssaisi'} Users) \tag{4.1}$$

  La requête 4.1 est très complexe mais peut être réduite en appliquant la règle de réécriture numéro 3. Nous obtenons le résultat suivant :

$$\sigma_{nomuser='nomsaisi'}(\sigma_{motpass='motdepasssaisi'} Users) \tag{4.2}$$

  Disons que les requêtes 4.1 et 4.2 renvoient les mêmes résultats mais peuvent avoir un impact différent quant à la performance du temps d'exécution. 4.1 exige qu'on puisse parcourir la relation Users deux fois alors que 4.2 une seule fois. Lorsque la relation Users contient un nombre élevé de tuples, il est recommandé d'utiliser la requête 4.2 pour espérer avoir une performance dans le temps d'exécution de la requête. Signalons que dans la suite, nous aurons à présenter uniquement la requête en algèbre relationnelle dans sa forme la plus simpliste que possible.

– Après une connexion réussie, le système identifie la prison à laquelle appartient l'utilisateur et filtre les données spécifiques à la prison. Par exemple, afficher la liste de tous les détenus se trouvant à la prison centrale de Bukavu :

$$\sigma_{nomprison='PCBUKAVU'}(Prison) \bowtie Prisonnier \tag{4.3}$$

– En plus de ce filtrage, le système identifie le type d'utilisateur pour afficher un menu adaptatif. Afficher le type d'utilisateur qui vient de se connecter pourra être réalisé comme la précédente requête.

Disons que la plupart de nos requêtes SQl seront conçues avec le formalisme de 4.1 et/ou 4.3. Certaines pourront utilisées même la forme généralisée de 4.3 faisant intervenir plusieurs relations. Le but pour cette partie était de choisir une forme très simpliste de la requête SQl en l'analysant sous l'angle algèbre relationnelle.
Nous pouvons présenter d'autres requêtes SQl avec leurs expressions équivalentes en algèbre relationnel de la manière suivante :

– Selection
  1. Liste de tous les prisonniers de sexe masculin

     select * from prisonnier where sexe='m' ;

     $$\sigma_{sexe='m'}(prisonnier)$$

  2. Liste de prisonniers de religion catholique

     select * from prisonnier join religion on prisonnier.idreligion=religion.idreligion where religion='catholique' ;

     $$\sigma_{nomreligion='catholique'}(prisonnier) \bowtie_{idreligion} religion$$

– Projection
  1. Affichage du nom, postnom des prisonniers dont l'adresse est bagira

     select nom, postnom from prisonnier where adresse='bagira' ;

     $$\pi_{nom,postnom}(\sigma_{adresse='bagira'}(prisonnier))$$

  2. Affichage du nom de la prison où est affecté le personnel du nom de Jean

     select nomprison from prison join personnel on prison.codeprison=personnel.codeprison where personnel.nom='jean'

     $$\pi_{nomprison}(\sigma_{personnel.nom='jean'}(prison) \bowtie_{codeprison} personnel)$$

– Union
  1. Affichage du nom, postnom des prisonniers dont l'adresse est bagira OU ibanda

     select nom, postnom from prisonnier where adresse='bagira'UNION select nom, postnom from prisonnier where adresse='ibanda' ;

     $$\pi_{nom,postnom}(\sigma_{adresse='bagira'}(prisonnier)) \cup \pi_{nom,postnom}(\sigma_{adresse='ibanda'}(prisonnier))$$

2. La requête précédente peut encore être réécrite de la façon suivante :

$$\pi_{nom,postnom}(\sigma_{adresse='bagira' \bigvee adresse='ibanda'}(prisonnier))$$

- Intersection
  1. Affichage du nom, postnom des prisonniers dont l'adresse est bagira et de sexe masculin

     select nom, postnom from prisonnier where adresse='bagira' INTERSECT select nom, postnom from prisonnier where sexe='M' ;

     $$\pi_{nom,postnom}(\sigma_{adresse='bagira'}(prisonnier)) \cap \pi_{nom,postnom}(\sigma_{sexe='M'}(prisonnier))$$

  2. La requête précédente peut encore être réécrite de la façon suivante :

     $$\pi_{nom,postnom}(\sigma_{adresse='bagira' \bigwedge sexe='M'}(prisonnier))$$

- Différence
  1. Affichage du nom, postnom des prisonniers dont l'adresse n'est pas celle de bagira

     select nom, postnom from prisonnier EXCEPT select nom, postnom from prisonnier where adresse='bagira' ;

     $$\pi_{nom,postnom}(prisonnier) - \pi_{nom,postnom}(\sigma_{adresse='bagira'}(prisonnier))$$

  2. Affichage des prisons se trouvant dans une province autre que celle du sud-kivu

     select nomprison from prison join province on prison.idprovince=province.idprovince EXCEPT
     select nomprison from prison join province on prison.idprovince=province.idprovince where province.nomprov='SUD-KIVU'

     $$\pi_{nomprison}(prison \bowtie_{idprovince} province) -$$

     $$\pi_{nomprison}(\sigma_{province.nomprov='SUD-KIVU'}(prison) \bowtie_{idprovince} province)$$

- Produit Cartésien
  1. Affichage du produit cartésien entre la table province et prison

     select * from prison, province ;

     $$prison \times province$$

  2. Affichage du produit cartésien entre la table prisonnier et religion

     select * from prisonnier, religion ;

     $$prisonnier \times religion$$

- Jointure

1. Affichage des prisonniers de religion Protestante

   select * from prisonnier join religion on prisonnier.idreligion=religion.idreligion where religion='protestant' ;

$$\sigma_{nomreligion='protestant'}(prisonnier) \bowtie_{idreligion} religion$$

2. Affichage du nom de la prison ainsi que de la cellule du prisonnier 'MANENO'

   select nomprison, libelle from prisonnier join cellule on prisonnier.idcellule=cellule.idcellule Join prison on cellule.idprison=prison.idprison where prisonnier.nom='MANENO' ;

$$\pi_{nomprison,libelle}(\sigma_{prisonnier.nom='MANENO'}(prisonnier \bowtie_{idprison} cellule \bowtie_{prison}))$$

– Renommage

1. Renommage de l'attribut 'nomprison' de la table prison en designationPrison

   select idprison, idtype, idprovince, nomprison as designationPrison from prison ;

$$\propto [nomprison : designationPrison]prison$$

2. Renommage de l'attribut 'nomreligion' de la table religion en croyance

   select idreligion, nomreligion as croyance from religion ;

$$\propto [nomreligion : croyance]religion$$

– Division

1. Liste d'Infractions commises par tous les détenus

   select idinfraction from commettre Group By idinfraction Having count(*)=(select count(*) from prisonnier) ;

$$R1 = \pi_{idinfraction,idprisonnier}(commettre)$$
$$R2 = \pi_{idprisonnier}(prisonnier)$$
$$Resultat = R1 \div R2$$

2. Liste des sanctions ayant été appliquées à tous les prisonniers
   select idsanction from purger Group By idsanction Having count(*)=(select count(*) from prisonnier) ;

$$R1 = \pi_{idsanction,idprisonnier}(purger)$$
$$R2 = \pi_{idprisonnier}(prisonnier)$$
$$Resultat = R1 \div R2$$

4.3 Conclusion au chapitre sur le modèle mathématique

Les mathématiques fournissent des outils puissants pour la résolution des divers problèmes. L'organisation ainsi que le traitement des données sur ordinateur bénéficient pour leur mise en œuvre un cadre mathématique appelé Algèbre relationnelle. Ce formalisme est à la base du fonctionnement des tous les SGBD. Ces derniers sont des programmes informatiques qui permettent la manipulation et la création des données dans des structures appelées bases des données. Ils s'appuient sur le langage SQL. Le code SQL est traduit dans le code relationnel avec son exécution dans ces environnements. La plupart des solutions que nous préconisons dans ce présent travail consiste en l'élaborations des requêtes SQL. C'est pourquoi, il nous a été utile de les construire à la lumière de l'algèbre relationnelle. Ainsi, Nous avions présenté dans ce chapitre les opérateurs de l'algèbre relationnelle, les règles de réécritures et enfin la manière dont nous avions réalisée nos propres requêtes en vue d'obtenir une performance en termes de temps d'exécution et d'espace de stockage.

Chapitre 5

SÉCURISATION DU NOUVEAU SYSTÈME DE GESTION DU SYSTÈME PÉNITENTIAIRE DE LA RDC

5.1 Introduction

Un système informatique sans sécurité est comparable à une maison sans porte. Toute personne mal intentionnée peut y accéder et faire tout ce qu'il veut. Le système réalisé étant donné qu'il sera en ligne peut être vulnérable à des attaques si on ne le sécurise pas. Ces attaques peuvent conduire à la non disponibilité , non intégrité et à la non confidentialité des données. Il existe plusieurs mécanismes de sécurisation d'un système informatique. Nous avions choisi une sécurisation par mot de passe avant d'entrer dans le système. Malheureusement ce type de protection marche à moitié ; puisque face aux hackers avisés, il peut se manifester faible et facilement cassable. En vue de renforcer la sécurité par ce type de protection, nous préconisons crypter le mot de passe par un algorithme RSA.

5.2 Objectifs de la sécurité

Nous pouvons définir les objectifs de la sécurité informatique comme suit :[18][21]
- intégrité : Le critère d'intégrité est relatif au fait que des ressources, données, traitements, transactions ou services n'ont pas été modifiés, altérés,ou détruits tant de façon intentionnelle qu'accidentelle. L'information ne sera modifiée que par les personnes autorisées.
- confidentialité : Le critère de confidentialité exige que l'information qui se trouve dans le système soit lue que par des personnes autorisées.
- disponibilité : Le critère de disponibilité exige que l'information qui se trouve dans le système soit disponible à tout moment aux personnes autorisées.
- non-répudiation : Le critère de non-répudiation exige qu'une transaction ne puisse être niée ou rejetée si elle a eu lieu.
- authentification : Le critère d'authentification consiste à assurer que seules les personnes autorisées aient accès aux ressources.

Tous ces aspects de sécurité ont été pris en compte dans notre projet d'une manière ou d'une autre en utilisant à bon escient la notion des sessions dans la programmation et les fonctions de

hachage. Néanmoins, un accent particulier a été placé sur les principes d'authentification et de confidentialité où le chiffrement RSA a été utilisé.

5.3 Mécanismes de sécurité

Il existe plusieurs mécanismes de sécurité :[19][20]
- Le chiffrement : est la transformation d'un message dit clair en un message chiffré dit cryptogramme. Cette transformation porte encore le nom de cryptage.
- Signature numérique : consiste à utiliser un chiffrement particulier appelé chiffrement irréversible. Celui-ci transforme un message en un bloc de données tel qu'il est impossible de reconstruire le message à partir du bloc. Les algorithmes utilisés sont appelés fonction de hashage ou fonction de condensation. Le bloc est appelé condensé ou signature. Les plus connus sont MD5(Message Digest5) et SHA1(secure Hash Algorithm1).
- Mots de pass : Lorsque les entités homologues et les moyens de communication sont surs, l'identification des entités homologues peut se faire par un identificateur(login) et un mot de passe.
- Liste de contrôle d'accès : Le mécanisme des listes de controle d'accès utilise l'identité authentifiée des entités et des informations fiables pour déterminer leurs droits d'accès au réseau ou aux ressources sur le réseau.
- etc.

Précisons tout de même que :[20][23]

Définition 5.1 *La cryptographie est un terme générique, désignant l'ensemble des techniques permettant de chiffrer des messages. Le verbe crypter est parfois utilisé mais on lui préférera le verbe chiffrer.*

Définition 5.2 *La cryptanalyse, à l'inverse est l'étude des procédés cryptographiques dans le but de trouver des faiblesses, en particulier, de pouvoir décrypter des messages chiffrés.*

Définition 5.3 *Le decryptement est l'action consistant à trouver le message en clair sans connaitre la clé de déchiffrement.*

Définition 5.4 *La clé est un paramètre partagé entre l'émetteur et le récepteur et implémente dans les opérations de chiffrement et de déchiffrement.*

Définition 5.5 *La cryptologie englobe la cryptographie et la cryptanalyse.*

Définition 5.6 *Un cryptosystème est un terme utilisé en cryptographie pour désigner un ensemble composé d'algorithmes cryptographiques et de tous les textes en clair, textes chiffrés et clés possibles.*

5.4 Cryptographie

5.4.1 Introduction

La cryptographie est l'art de rendre inintelligible, incompréhensible, de crypter, de coder, un message pour ceux qui ne sont pas habilités à en prendre connaissance. Elle assure ainsi la confidentialité, l'authenticité et l'intégrité des messages. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret.

5.4.2 Historique

Les premières utilisations de la cryptographie remontent à l'antiquité, notamment avec le chiffre de César, en référence à Jules César, qui l'utilisait pour protéger ses communications. Mais la cryptographie est bien plus ancienne que cela. Ce domaine, il y a quelques années était réservé au domaine militaire et aux grandes entreprises. C'est souvent lors de la transmission des messages dans l'armée pendant les premières guerres mondiales que ce besoin est née de ne pas être écouté par ses ennemis. Il fallait un moyen de transmettre secrètement les informations sur les champs de bataille.

5.4.3 Types de cryptographie

Il existe deux grands types de cryptographies : [23]

Cryptographie à clé symétrique

On parle de la cryptographie symétrique lorsque la même clé est utilisée pour crypter et décrypter le message. Le problème de ce cryptage est que lorsqu'on a N personnes qui doivent communiquer ; on doit avoir à s'échanger (N*(N-1)/2) clés. Nous remarquons que plus le nombre de personnes augmente, plus la gestion des clés devient très fastidieuse. Aussi il faudrait alors énormément de ressources pour que deux clés ne soit pas identiques. C'est pourquoi, dans les années 1970, la cryptographie asymétrique a été mise au point par Whitfiel Diffie et Martin Hellman.

Cryptographie à clé asymétrique

Dans le but de résoudre le problème due au cryptage symétrique, les ténors de cette approche voudrons que le principe de fonctionnement repose sur une paire de clés privée et publique. La seconde étant dérivée de la première et peut être distribuée à n'importe qui. Tandis que l'autre doit être tenue secrète. Dans ce cas le message est chiffré avec la clé publique et déchiffré avec la clé privée. L'une des applications du principe de la cryptographie à clé asymétrique est la cryptographie par RSA.

Notre choix s'est porté au cryptosystème RSA parce que, premièrement il est incassable et deuxièmement il répond bien au but que nous cherchons, celui de rendre incompréhensible l'information transmise au serveur. La notion d'incassabilité de cet algorithme se base principalement sur la difficulté de factorisation d'un grand nombre premier en ses facteurs. Les détails du fondement de cet algorithme sont fournis dans les suivantes sections.

5.5 Cryptographie par RSA

Le système de cryptage RSA a été inventé en 1978 par Ron Rivest (Cryptologue américain), Adi Shamir (Expert en cryptanalyse israélien) et Len Adleman (Chercheur en informatique et biologie moléculaire américain), d'où le sigle RSA[14].

5.5.1 Usages de RSA

- On l'utilise notamment dans les transactions sécurisées sur internet ;
- Le RSA est aussi implanté dans les systèmes d'exploitation de Sun, Apple, Microsoft et Nobel ;
- Le RSA est intégré dans les cartes Ethernet, les Cartes à puce Bancaires ;
- Un grand nombre d'institutions gouvernementales, militaires et universitaires l'utilise.

5.5.2 Description de l'algorithme RSA

Alice veut envoyer un message M à Bob[15].
- M un entier représentant un message.
- Bob choisit p et q deux nombres premiers et on note n leur produit.
- Bob choisit e un entier premier avec $p-1$ et $q-1$.
- On a $\phi(n) = (p-1)(q-1)$ donc e est premier avec $\phi(n)$ et on obtient (via Bézout) qu'il est inversible modulo (n) ; i.e. il existe un entier d tel que $ed \equiv 1(mod\phi(n))$.
- Le message chiffre sera alors représente par : $C = M^e(mod(n))$
- Pour déchiffrer C ; on calcule d l'inverse de $emod\phi(n)$;
- ensuite on calcule $C^d modn$:

5.5.3 Exemple d'application

On choisit d'illustrer l'algorithme sous forme d'un exemple simple[14] :
On prend deux nombres premier : p = 47 et q = 71
On calcul n = p*q = 47 * 71 = 3337
(p-1)(q-1) = 3220
e = 79 (démonstration avec le Théorème de Bezout)
On calcul d = = 1019 On vérifie que e*d = 80501 = 1 mod 3220
Prenons un message préalablement transformé en nombre grâce par exemple à la table ASCII
m = 6882326879666683
On découpe m : m1=688 m2=232 m3=687 m4=966 m5=668 m6=3
On calcul chaque bloc : $c_x = m_x^e modn$ (Grace a au couple (e,n), clé publique)
On trouve c1=1570 c2=2756 c3=2091 c4=2276 c5=2423 c6=158
Le message crypter est donc : c = 157027562091227624231 58
On retrouve m en calculant $m_x = c_x^d modn$ (Grace a au couple (d,n), clé privé)
Ainsi nous remarquons que cet algorithme comprend 3 grandes étapes :
- la génération des clés
- le chiffrement
- le déchiffrement

5.5.4 Quelques failles de RSA

- L'opération de cryptage est déterministe, ce qui permet à un attaquant, connaissant la valeur cryptée, à rechercher le texte en clair correspondant à celle-ci.
- L'exponentiation modulaire est malléable, étant donné le «cryptage» de m1 et m2, une simple multiplication donne le cryptage de m1m2. Cela s'apparente au cryptage homomorphe, qui peut être une bonne propriété, ou non, selon le contexte.
- L'attaque par diffusion : Lorsque le même message est envoyé à au moins u différents correspondants, il peut être retrouvé(avec une forte probabilité) sans connaître la clé privée.[17]

Ces différentes attaques sont réalisées à partir de la valeur cryptée de l'algorithme RSA. Comment renforcer la sécurité de l'algorithme RSA lui-même ? Une des améliorations de RSA est Optimal Asymmetric Encryption Padding, qui consistera à cacher à son tour la valeur cryptée par des opérations de hachage avec xor et d'ajout d' une valeur générée aléatoirement au message chiffré. C'est cette version qui est utilisée dans le présent package.

5.5.5 Application de l'algorithme RSA-Optimal Asymmetric Encryption Padding dans notre projet

Rappelons tout d'abord que notre système a été déployé selon une approche client-serveur. Nous comptons proposer dans cette section, un moyen efficace pour envoyer le mot de passe saisi par un client du système vers le serveur. Nous allons utiliser l'algorithme RSA pour crypter le mot de passe afin qu'il soit inintelligible au moment de sa transmission vers le serveur. Ainsi, ce mot de passe sera crypté au moyen du langage Java Script (coté client) et décrypté au moyen du langage PHP (coté serveur). Nous pouvons illustrer ce processus grâce au menu "user" puis "test RSA" de l'utilisateur "administrateur". Nous obtenons l'écran suivant :

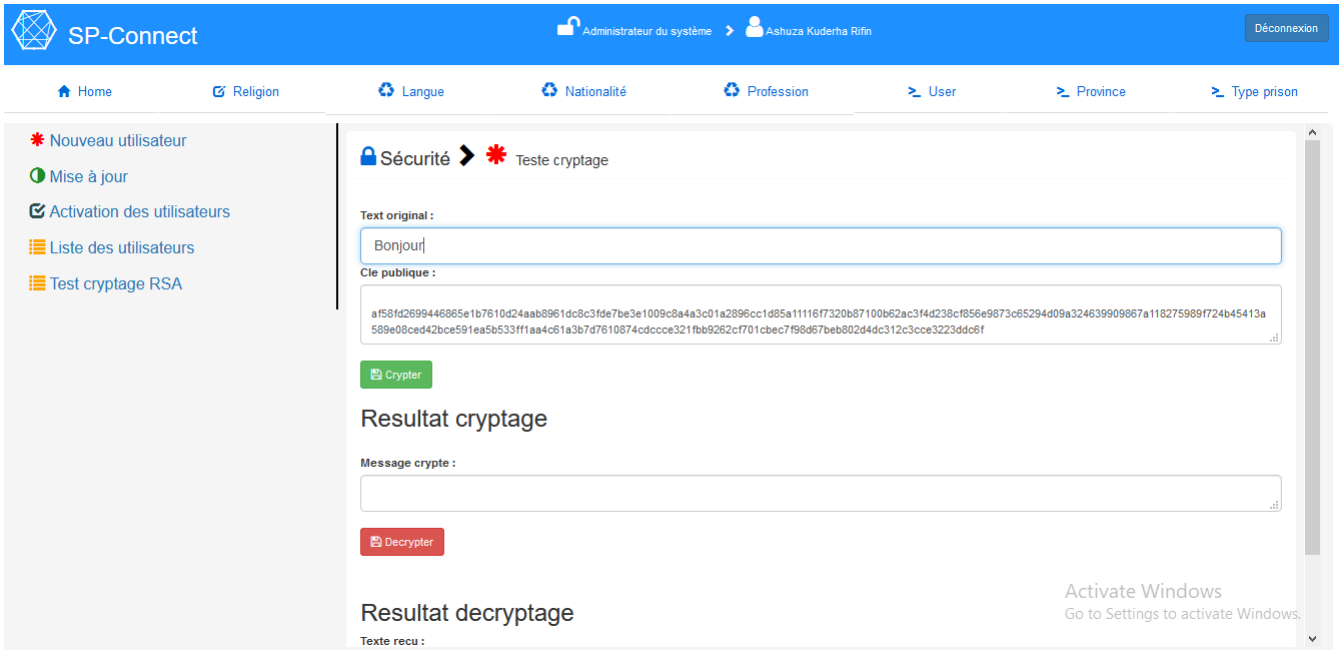


FIGURE 5.1 – Interface d'illustration du cryptage RSA

Sur cette figure en cliquant sur le bouton "Crypter", on obtient l'écran suivant :

Le message crypté sur cette figure est l'information qui sera transmise vers le serveur pour que ce dernier puisse le décrypter. L'opération de cryptage coté client a été réalisé en utilisant la clé publique du serveur. Comme on peut le remarquer, la clé privée du serveur n'est pas visible sur cet écran. Pour dire que c'est une information qui reste toujours cachée par le serveur. Au moment du décryptage, nous obtenons la figure suivante en cliquant sur le bouton décrypter".

Ce processus illustre ce qui se passe du coté serveur lorsque le mot de passe déjà crypté lui est envoyé par le client. Nous avions utilisé le package de l'université de MIT sous licence que nous avions adapté pour résoudre notre problème. Pour ce package, il y a génération d'une clé générale codée sous le format base64 qui contient toutes les informations sur les différents paramètres de l'algorithme RSA comme vu précédemment.

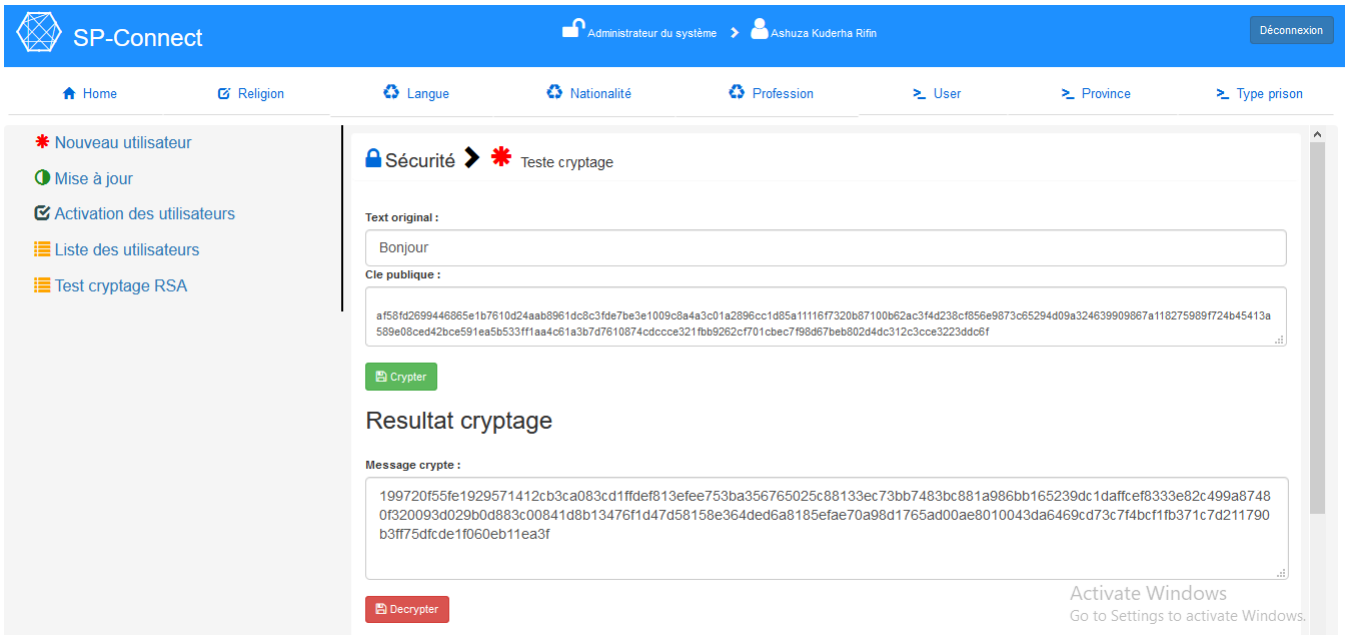


FIGURE 5.2 – Résultat du cryptage

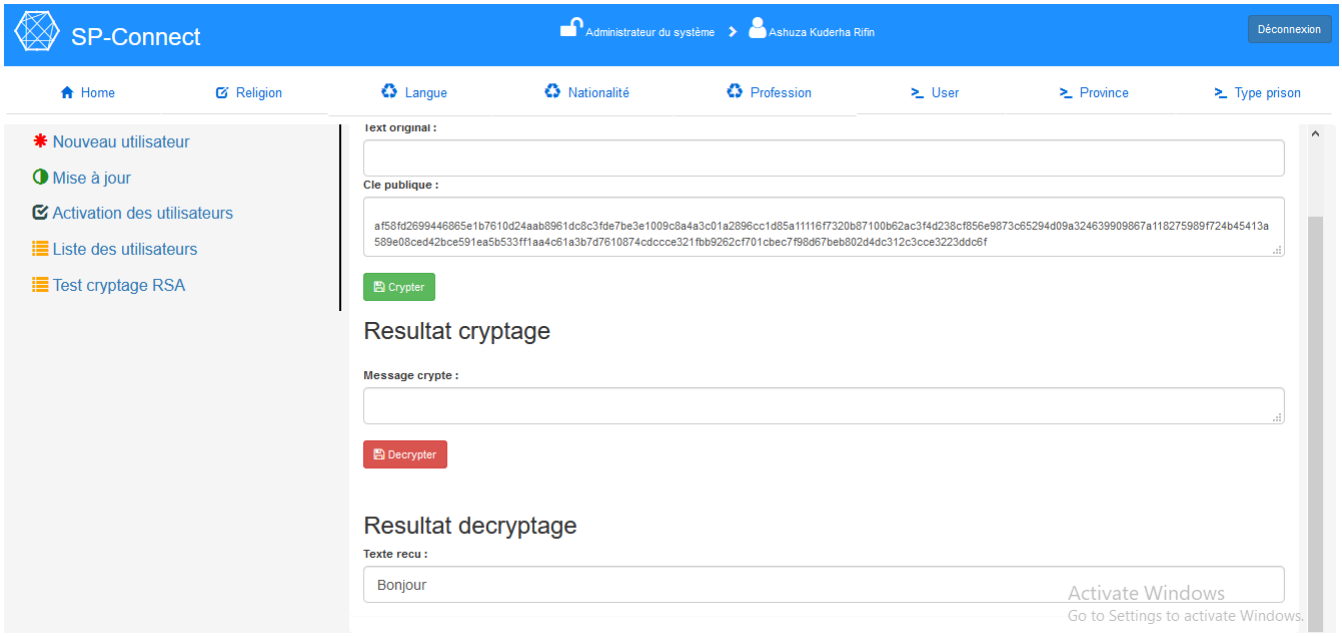


FIGURE 5.3 – Résultat du décryptage

L'aspect important de ce package est l'utilisation des valeurs des paramètres de l'algorithme de RSA sous forme hexadécimal ou base 64. Cela permet aussi de réduire la quantité d'information à transmettre sur réseau lorsqu'on manipule de très grand nombre comme c'est le cas en RSA. C'est la raison qui nous a poussé à utiliser ce package. Pour plus de précision, nous avions montré à la figure 5.4, comment se présente les différentes valeurs de paramètres de RSA fourni par ce package.

Enfin, il est très important de remarquer sur cette petite démonstration, qu'au moment du cryptage d'un mot, la page ne se charge pas mais le contraire au moment du décryptage. Cela prouve que le cryptage se fait du coté client(JavaScript) et le décryptage du coté serveur(php).

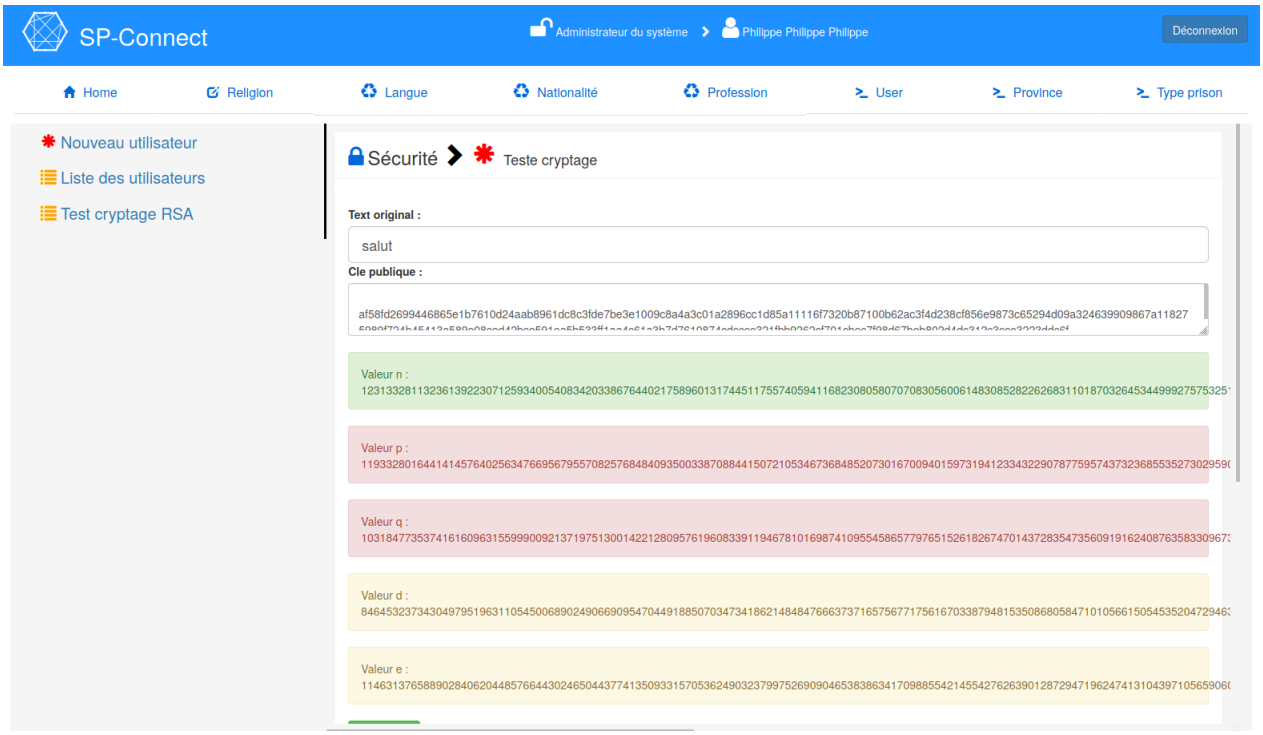


FIGURE 5.4 – Valeurs de paramètres RSA

5.5.6 Données Test

Dans cette section, nous allons préciser le mécanisme que nous avions utilisé pour le partage des données des identifiants en vue de l'utilisation du système.

Pour ce faire nous avions utilisé, l'algorithme césar pour chiffrer toutes les données à partager. Ensuite, nous avions chiffré la clé du césar par l'algorithme RSA. Il s'agit, en effet d'une cryptographie mixte.
Pour commencer nous avions chiffré la clé césar avec les valeurs suivantes :

Table 5.1 – Valeur paramètre RSA

p	160341381751510701521179014646168742190926312422811086246263078637860578883475645080256760387588302981609518450850786273910179929878946630067098490579758428637672887733937503778632378834496397396778152369526653021773434882810500012239520969111347107785082833095177068743593424934849977400686810338773427842163
q	142604740402940070817095076613402730969721463105334112211167489206740067014451680374347561464350771904731823273263584681243112967579166624039552453346397295158682799086030057439723328594013022521411690050209460416032338990224442861381871688181653886244847149528574194709188882012056972488829054932228643399729
e	102886604922422796852115440605790289249845646217694506482484783519958790403795060204256659952922643132834596643283445571634927310813929429783940764138366667
clé césar	181136896411412052938873721001847162539554208610707302079179922275190905502528151907911579869851276811062837204935645524534485873669701577591430420306124534686893298260649582220184184004207781814309773616024477871993366961113275193785605561815065178836639908616089077349109869410680297950227931541366162089794012526313695229387169712167423193647805013977474545490723064289980956817551092150866889596906059782553078363444850137264120039517345426631921612230123113851904499876037243953805930391086966690221565156210395097469572904877106281864276959033872159874412939559572339159162213146970370654303830733226267529328 34

*$)&à%&4à*%&/5*'*"/54à%Ï"$$&4à41$0//&$5ÊÊ

*&/úÊÊ888î41$0//&$5î"3&5/î$%

:1&Ê	3*40/à%ç""&$5"5*0/Ê	%&/5*'*"/54ÊÊÊ
3&"*&3ÊÊ	3*40/à%&à "#"3&Ê	4&3/".& ú30."*/ "44803%ú30."*/
	3*40/à%&à","-"Ê	4&3/".&ú1)*- *11&Ê"44803%ú1)*-*11&
	3*40/à$&/53"-&à%&à6,"76Ê	4&3/".&ú(3&'"*&3Ê"44803%ú(3&'"*&3
*3&$5&63ÊÊ	3*40/à%&à "#"3&Ê	4&3/".&ú'*%&-&Ê"44803%ú'* %&-&
	3*40/à%&à","-"ÊÊ	4&3/".&ú-6#"-"Ê"44803%ú- 6#"-"
	3*40/à$&/53"-&à %&à6,"76ÊÊ	4&3/".&ú %*3&$5&63Ê"44803%ú %*3&$5&63
*/*45&3&à %&à-"à+645*$&ÊÊ		4&3/".&ú.*/ *45&3&Ê"44803%ú.*/ *45&3&
0-*$*&3ÊÊ %.*/*453"5&63à %6à4:45&.&ÊÊÊ		4&3à/".&ú,")"4)"Ê"44803%ú,") "4)"
%.*/*453"5&63à %6à4:45&.&ÊÊÊ		4&3à/".&úà"%.*/ Ê"44803%ú"%.*/

Figure 5.5 – Fichier Identifiant encrypté

Ce sont les données qui seront transmises au concerné par mail par exemple. Lorsqu'il les reçoit, il devra d'abord trouver la clé césar en clair en décryptant ce dernier par RSA. La valeur de la clé trouvée est de 192. Utiliser par exemple `https://www.dcode.fr/chiffre-rsa` en utilisant les valeurs du tableau 5.1 pour s'en convaincre. Prenez toutefois soin d'éviter d'espacer quand vous faites copier et coller. C'est avec cette valeur qui sera utilisée comme clé dans l'algorithme césar. En décryptant le fichier de la Figure 5.5, on obtient ce qui suit :

FICHE DES IDENTIFIANTS D'ACCES SPCONNECT

Lien : www.spconnect.aretn.cd

Type	Prison d'affectation	Identifiants
Greffier	Prison de Kabare	User name : romain Password : romain
	Prison de Makala	User name : philippe Password : philippe
	Prison centrale de Bukavu	User name : greffier Password : greffier
Directeur	Prison de Kabare	User name : fidele Password : fidele
	Prison de Makala	User name : lubala Password : lubala
	Prison centrale de Bukavu	User name : directeur Password : directeur
Ministère de la justice		User name : ministere Password : ministere
Policier		User name : kahasha Password : kahasha
Administrateur du système		User name: admin Password: admin

FIGURE 5.6 – Fichier Identifiant décrypté

Sur cette figure, nous constatons que les mots choisis sont dits faibles puisque facilement trouvable. Néanmoins, l'administrateur du système doit envoyer à un utilisateur un mot de passe faible pour lui permettre de se connecter facilement pour la première fois au système. Ce n'est qu'après une première connexion, qu'il sera appelé à se choisir un mot de passe fort, grâce au menu "comptes". Un mot de passe fort, c'est un mot de passe qui contient tous les types de caractères(exemple :PhilB052 !). C'est pour dire que les mots de passe choisis dans ce fichier identifiant sont établis seulement dans le cadre de Test du système et non pour l'utilisation durable.

5.6 Conclusion au chapitre sur la sécurisation du nouveau système

Le système étant déjà fonctionnel et exploitable ne suffit pas. Il faut ajouter une petite retouche en le sécurisant en vue d'assurer sa pérennité à long terme. Pour sécuriser notre système nous nous sommes appuyés sur deux aspects : la protection des droits d'accès aux données et opérations d'une part et l'accès au système grâce à une authentification sécurisée, d'autre part. Le premier aspect a été réalisé grâce à l'architecture MVC que nous avions adoptée pour la construction du système. En effet, avant d'accéder à une interface(view) pour manipuler les données et effectuer des traitements, un contrôleur(chef d'orchestre qui fait le lien entre données(modèle) et view) doit préalablement vérifier si vous en avez le droit. On a ainsi construit un menu adaptatif par rapport au type utilisateur. Pour le deuxième aspect, nous avions crypté le mot de passe par RSA pour le rendre inintelligible au moment de sa transmission au serveur, grâce à un package de l'université de Massachusetts Institute of Technology.

Chapitre 6

PRÉSENTATION DU FONCTIONNEMENT DE L'APPLICATION

6.1 Introduction

Dans ce chapitre nous faisons une description fonctionnelle du nouveau système conçu et réalisé et montrons les états qui sont générés. Rappelons que notre démarche de la mise en œuvre de ce système a été largement inspiré par le langage UML. Parmi les diagrammes élaborés, nous avons élaboré le diagramme de cas d'utilisation. Ce dernier donne les grandes fonctionnalités du système par acteur. la réalisation du système étant une matérialisation de ce qui a été conçu, nous allons présenter le fonctionnement de celui-ci à partir de chaque acteur. c'est pour ainsi dire que chaque acteur aura un menu propre à lui lorsqu'il se connecte pour qu'il puisse utiliser le présent système. Les différents acteurs sont : le Ministère de la justice, l'Administrateur du système, le Directeur de la prison, le greffier et enfin la Police. Dans un premier temps, nous allons présenter les fonctionnalités principales par acteur. Ensuite nous allons factoriser certains résultats clés obtenus puis suivra la présentation des différents rapports générés et enfin nous détaillerons le processus d'hébergement .

6.2 Connexion

Tous les acteurs sont obligatoirement appelés à fournir leurs identifiants (nom d'utilisateur et mot de passe) avant d'accéder au système. Cette fonctionnalité est commune à tous les utilisateurs. Sa fenêtre se présente de la manière suivante comme le montre la figure 6.1.

Comme ce système est sensé être utilisé dans toute la République Démocratique du Congo, après une connexion réussie, le système pourra identifier la prison à laquelle est affecté l'utilisateur qui vient de se connecter. Ceci dans le but de filtrer toutes les données relatives à la prison concernée. Étant donné que le système est multi-utilisateurs, ce dernier présente un menu adapté à chaque type d'utilisateur. Voyons maintenant les fonctionnalités de chaque utilisateur.

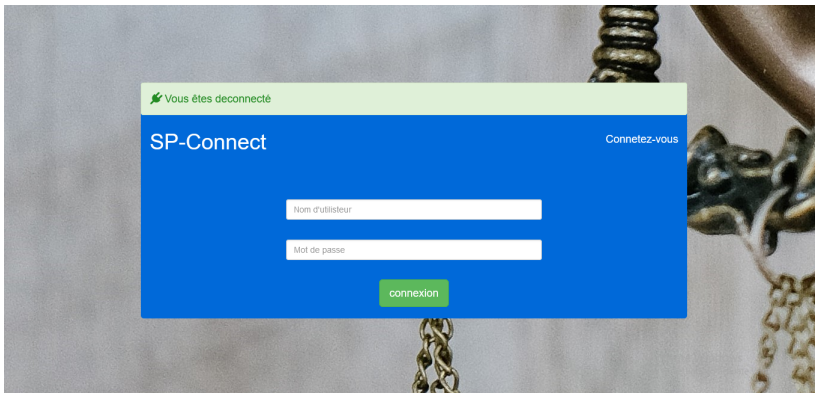


FIGURE 6.1 – Connexion

6.3 Analyse par acteur

6.3.1 Ministère de la Justice

Cet acteur est l'organe qui gère le personnel pénitentiaire (création,affectation, transfert, etc), fait le suivi de contrôle des dossiers et met en place des politiques générales sur les mécanismes de liberté conditionnelle. Il configure toutes les informations générales indépendantes d'une prison donnée. Il s'agit par exemple des informations sur les juridictions, les circonscriptions, les sanctions , les mesures disciplinaires, les prisons et les motifs de sortie. Son interface d'accueil se présente de la manière suivante :

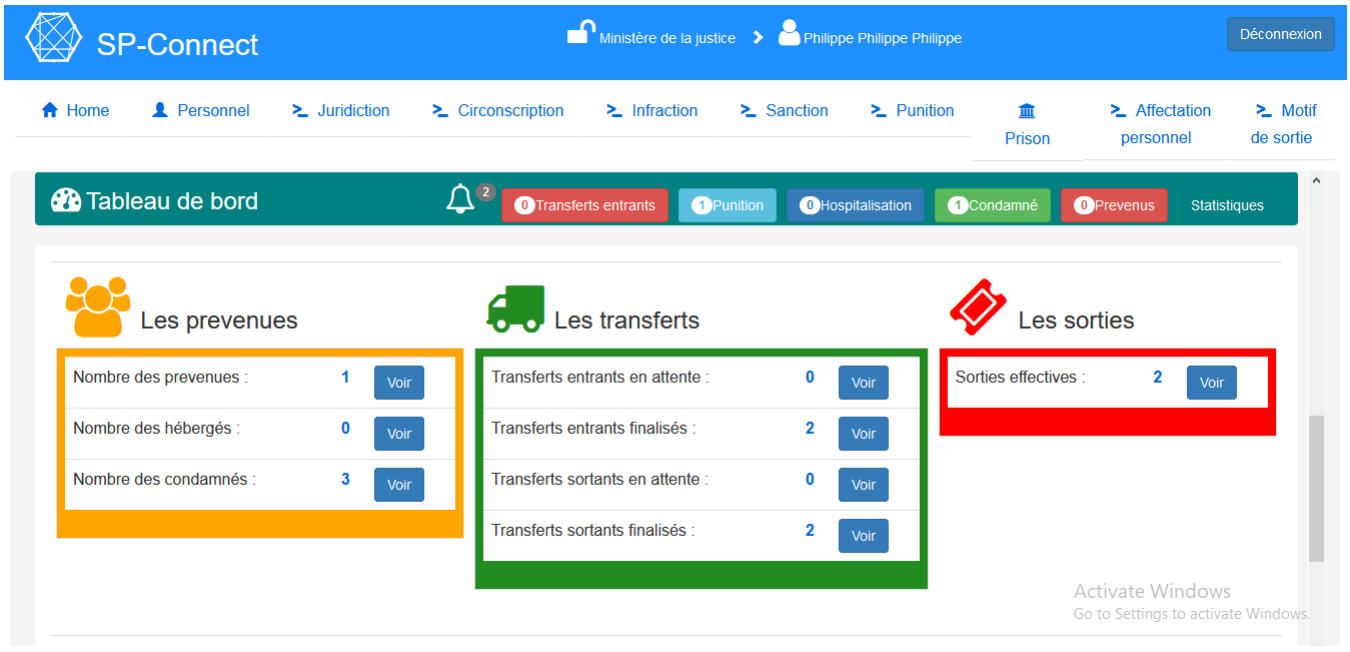


FIGURE 6.2 – Interface d'accueil du Ministère de la justice

Comme nous pouvons le constater sur cette interface, il peut créer un nouvel agent et l'affecter à une prison donnée. C'est bien lui qui complète toutes les informations liées aux infractions. Nous remarquons que c'est le Ministère de la justice qui a le droit d'effectuer les opérations CRUD sur toutes les entités dont il a la tâche de gérer. La partie 3 est un tableau de bord qui lui permet de visualiser tous les cas d'irrégularités observées dans différentes prisons.

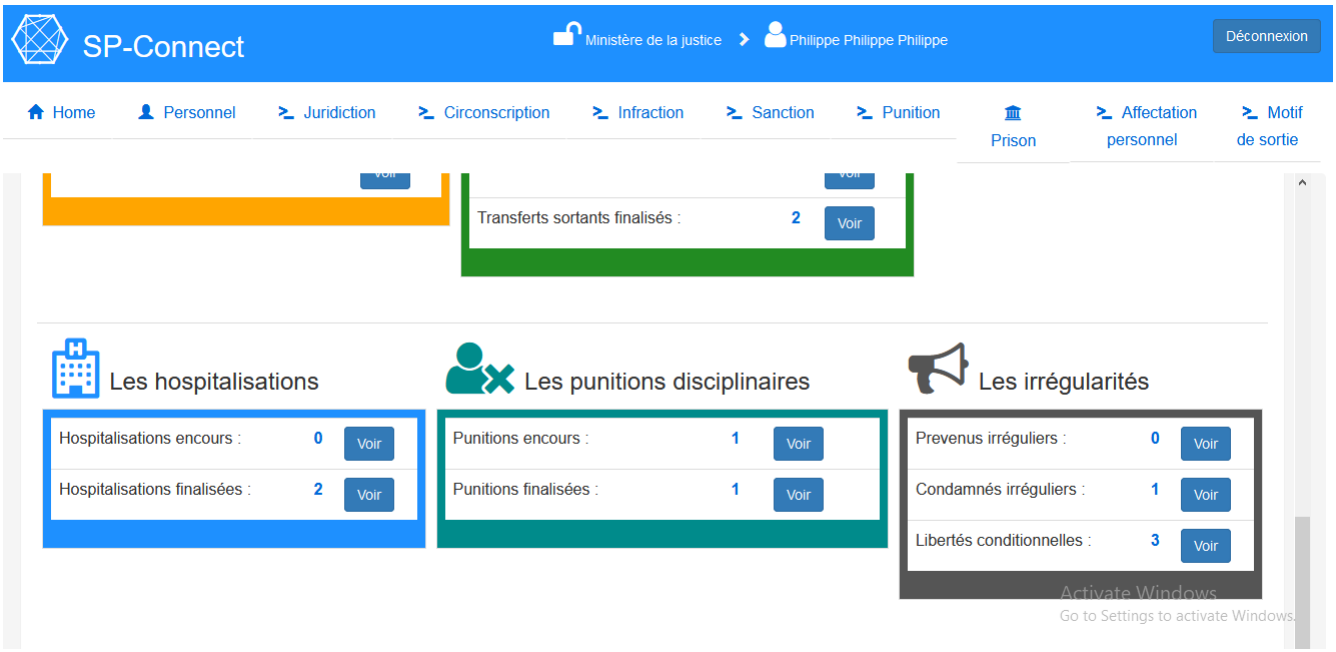


FIGURE 6.3 – Tableau de bord du Ministère de la Justice

Il peut aussi afficher les statistiques sur le nombre des détenus des différentes prisons.

6.3.2 Greffier de la prison

Les activités principales du Greffier de la prison sont de gérer les informations administratives du prisonnier ainsi que les tâches liées à la vie du prisonnier pendant son incarcération. Il s'agit de l'enregistrement du prisonnier, l'écrouement du prisonnier,l'enregistrement du jugement, le transfert des prisonniers vers une autre prison et la libération des prisonniers. Il sied de signaler que le contrôle de droit d'accès verrouille les accès du Greffier qu'aux seules informations auxquelles il a accès. Il s'agit ici des informations de la prison à laquelle il a été affecté. Après la connexion, un utilisateur du type "Greffier" est dirigé vers l'interface d'accueil du module des fonctionnalités du greffier. la figure suivante présente cette interface.

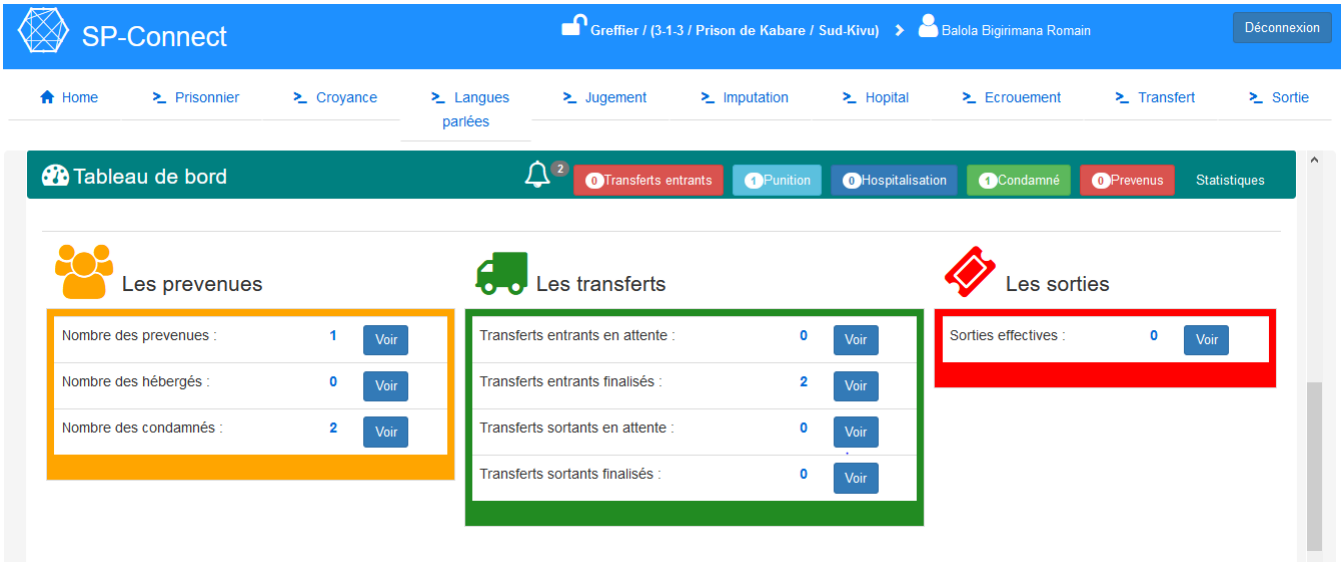


FIGURE 6.4 – Interface d'accueil du greffier d'une prison

Le parcours du prisonnier commence par l'enregistrement de ses informations administratives dans la base de données du système. L'interface ci-dessous nous permet d'effectuer cette opération d'enregistrement.

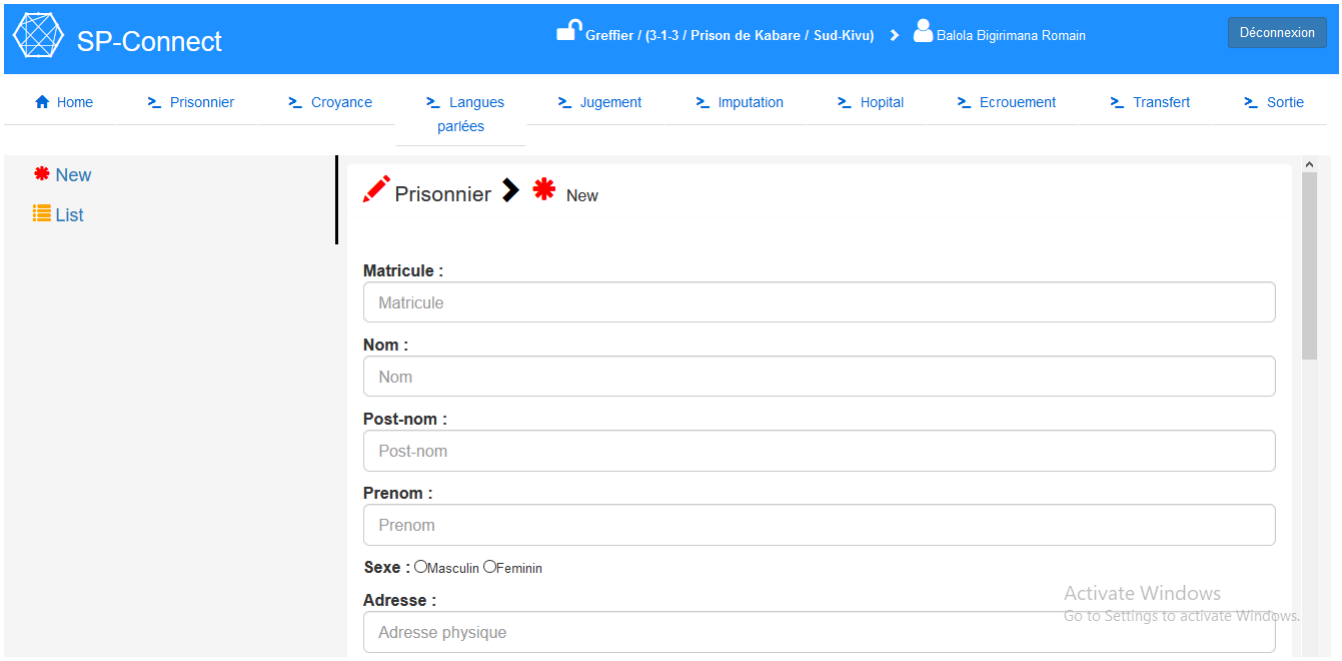


FIGURE 6.5 – Interface d'enregistrement d'un nouveau prisonnier

Après enregistrement du prisonnier, le Greffier enregistre alors son jugement suivi des peines prononcées. Chaque infraction commise par le prisonnier est liée à une sanction lui infligée. Une peine prononcée fait alors référence à une sanction donnée. L'interface suivante permet au Greffier d'enregistrer les peines relatives à un jugement donné prononcé contre un prisonnier.

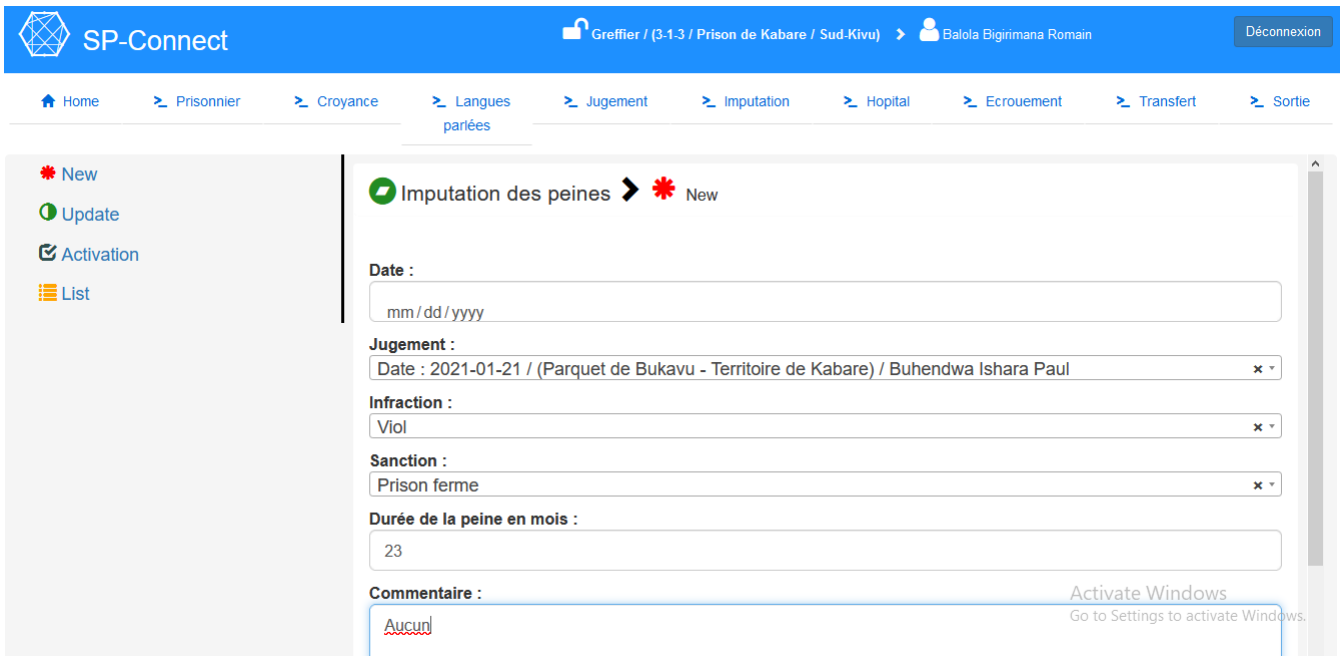


FIGURE 6.6 – Interface d'enregistrement des peines prononcées

La deuxième activité clé du Greffier c'est le transfert du prisonnier vers une autre structure pénitentiaire. Pour effectuer cette activité, il doit sélectionner un prisonnier et choisir la structure pénitentiaire dans laquelle ce dernier sera transféré. La figure suivante présente l'interface utilisée par le Greffier d'une prison pour effectuer le transfert d'un prisonnier.

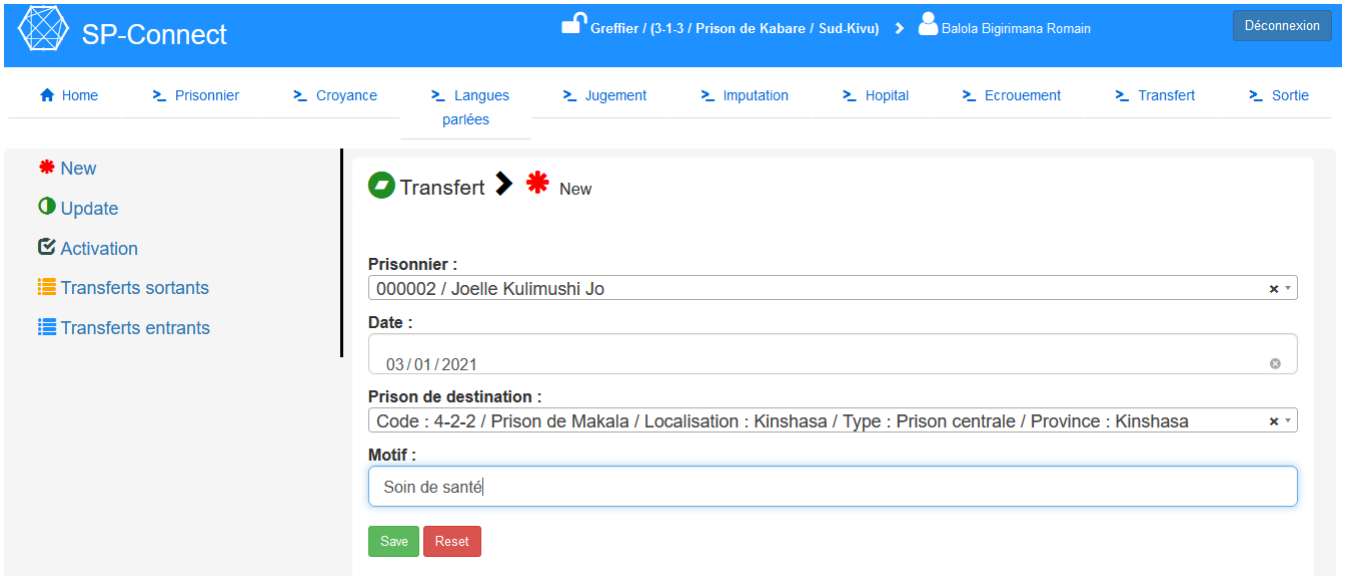


FIGURE 6.7 – Interface d'enregistrement du transfert d'un prisonnier

La troisième activité clé du Greffier consiste en l'enregistrement des libérations (sorties) des prisonniers. Cette libération peut avoir des motifs divers. Le système répertorie l'ensemble des motifs de sortie qui sont enregistrées au préalable par le Ministère de la Justice. La figure ci-dessous présente l'interface d'enregistrement d'une libération d'un prisonnier.



FIGURE 6.8 – Interface d'enregistrement d'une sortie (libération) d'un prisonnier

6.3.3 Directeur de la prison

Le Directeur de la prison est l'agent en contact direct avec le prisonnier. Dans le système, les activités du Directeur de la prison sont constitués par les tâches suivantes : l'affectation des pri-

sonniers dans les différentes cellules de la prison, le changement de cellule pour un prisonnier, l'enregistrement des hospitalisation pour les cas des maladies nécessitant une hospitalisation, l'enregistrement des informations d'une visite et l'enregistrement des mesures disciplinaires infligées contre un prisonnier donné. Comme pour le Greffier d'une prison, le Directeur d'une prison ne peut aussi qu'accéder aux informations propres à la prison dans laquelle il a été affecté ainsi qu'aux informations des prisonniers qui sont incarcérés dans cette même prison. Après s'être authentifié, le Directeur de la prison est dirigé vers le module des fonctionnalités exploitables par un utilisateur ayant le droit d'accès du type "Directeur de prison". La figure ci-dessous présente l'interface d'accueil du Directeur d'une prison.

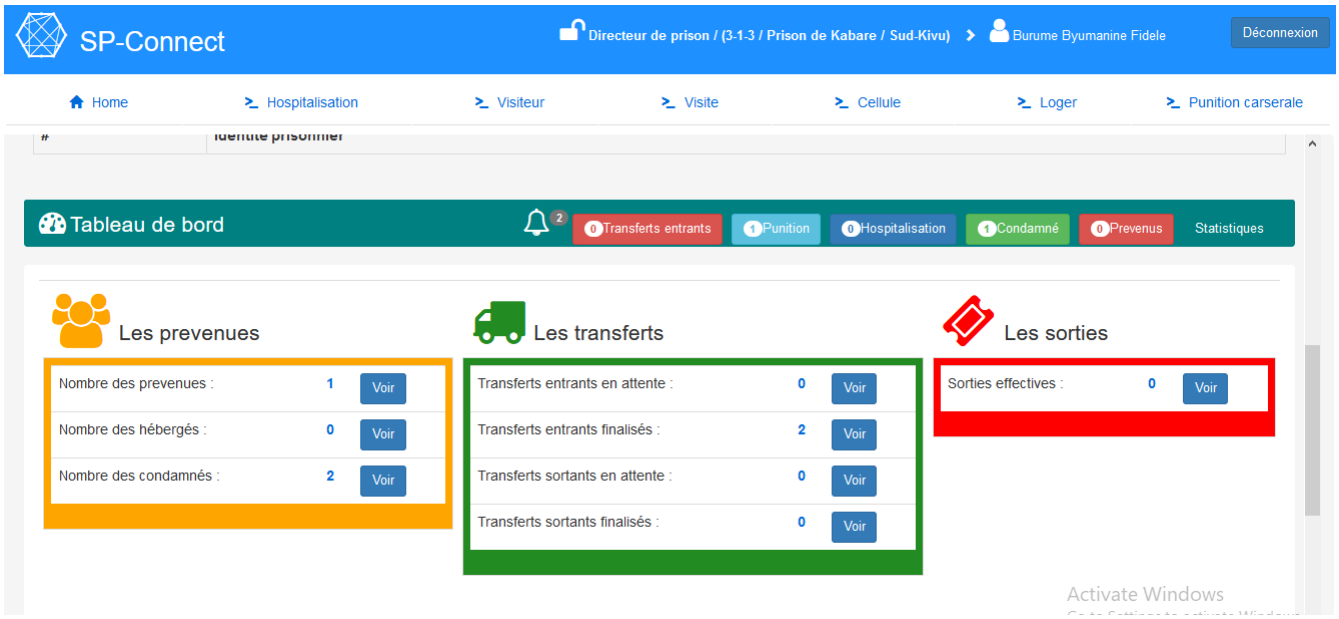


FIGURE 6.9 – Interface d'accueil du Directeur de prison

Quatre activités principales sont réalisées par le Directeur de prison. Chacune d'elles constitue une opération affectant le séjour du prisonnier dans la structure pénitentiaire. La première activité consiste en l'hospitalisation du prisonnier en cas de maladie nécessitant un séjour dans une structure de santé. Les structures de santé à utiliser dans le système sont enregistrées en amont par l'administrateur du système. D'autres informations concernant le séjour du prisonnier à l'hôpital sont aussi enregistrées. La figure ci-dessous représente l'interface d'enregistrement d'une hospitalisation.

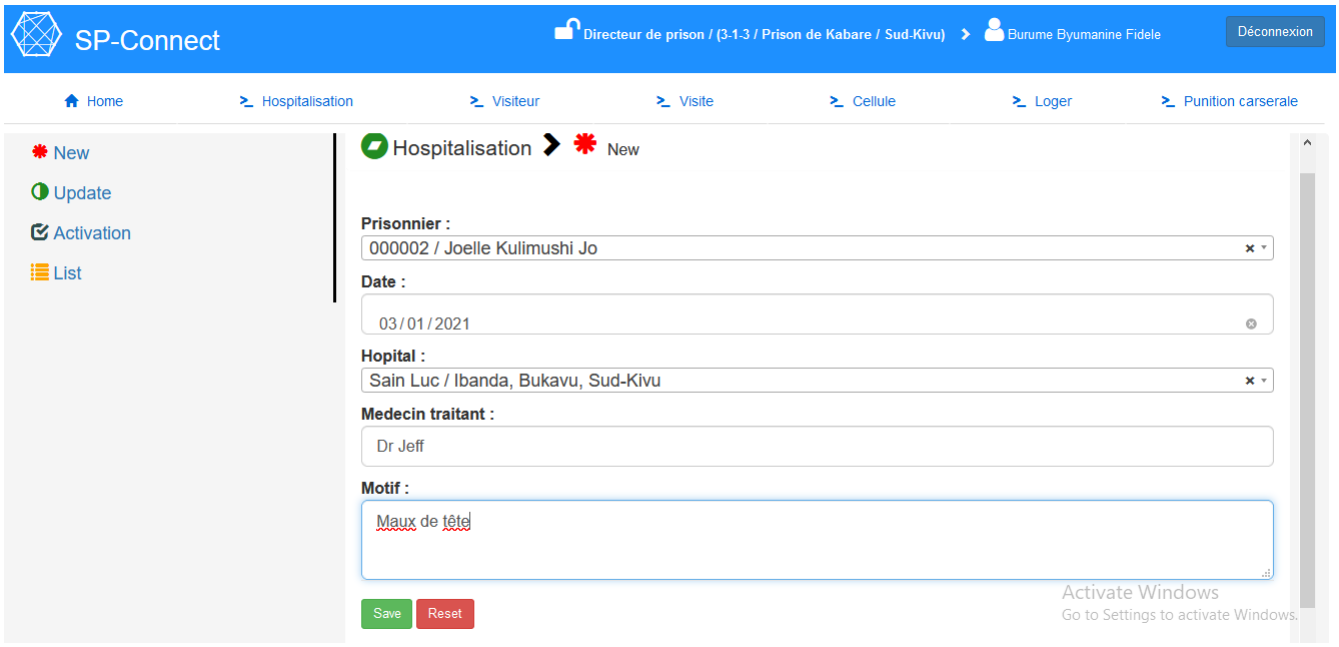


FIGURE 6.10 – Interface d'enregistrement d'une hospitalisation du prisonnier

La deuxième activité consiste en l'enregistrement des visites effectuées dans la prison. Pour chaque visite, le Directeur de la prison doit enregistrer les informations concernant l'identité du visiteur, le prisonnier qui sera visité, la date de la visite ainsi que le motif de la visite. La figure suivante représente l'interface d'enregistrement de la visite.

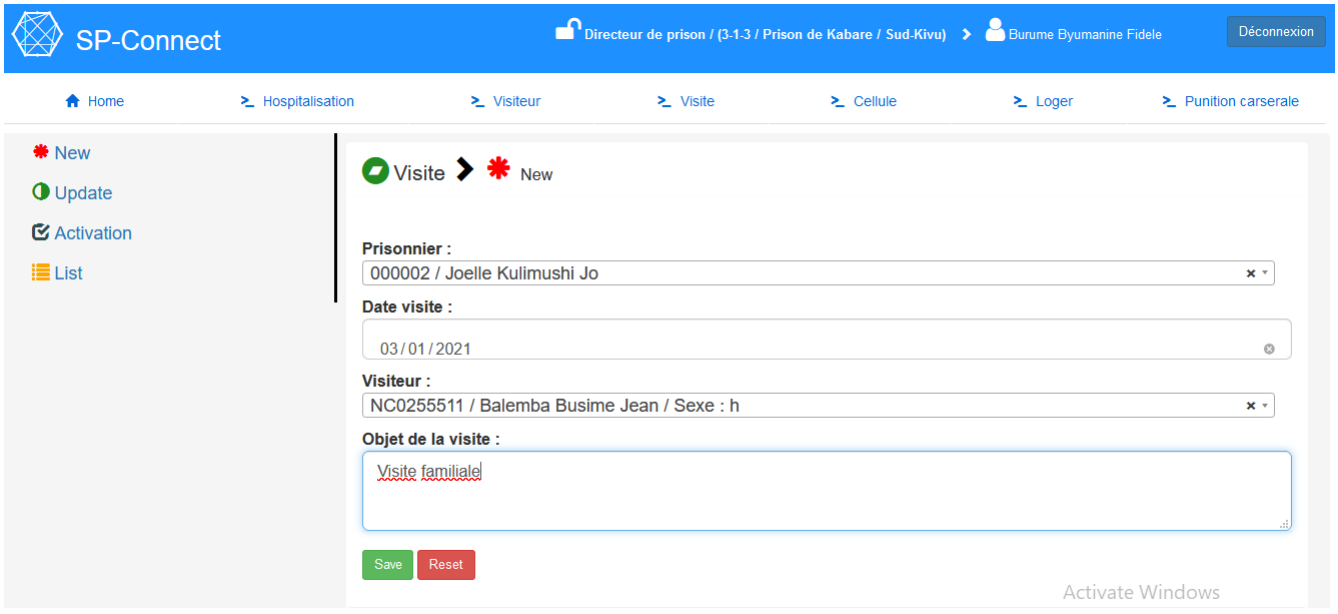


FIGURE 6.11 – Interface d'enregistrement d'une visite

L'avant dernière activité du Directeur de prison est l'affectation des prisonniers dans les différentes cellules de la prison. La première affectation d'un prisonnier dans une cellule s'effectue lors de l'ecrouement de celui-ci. En cas de nécessité, le prisonnier peut être alors affecté dans une autre cellule. La figure ci-dessous représente l'interface d'affectation des prisonniers dans les cellules.

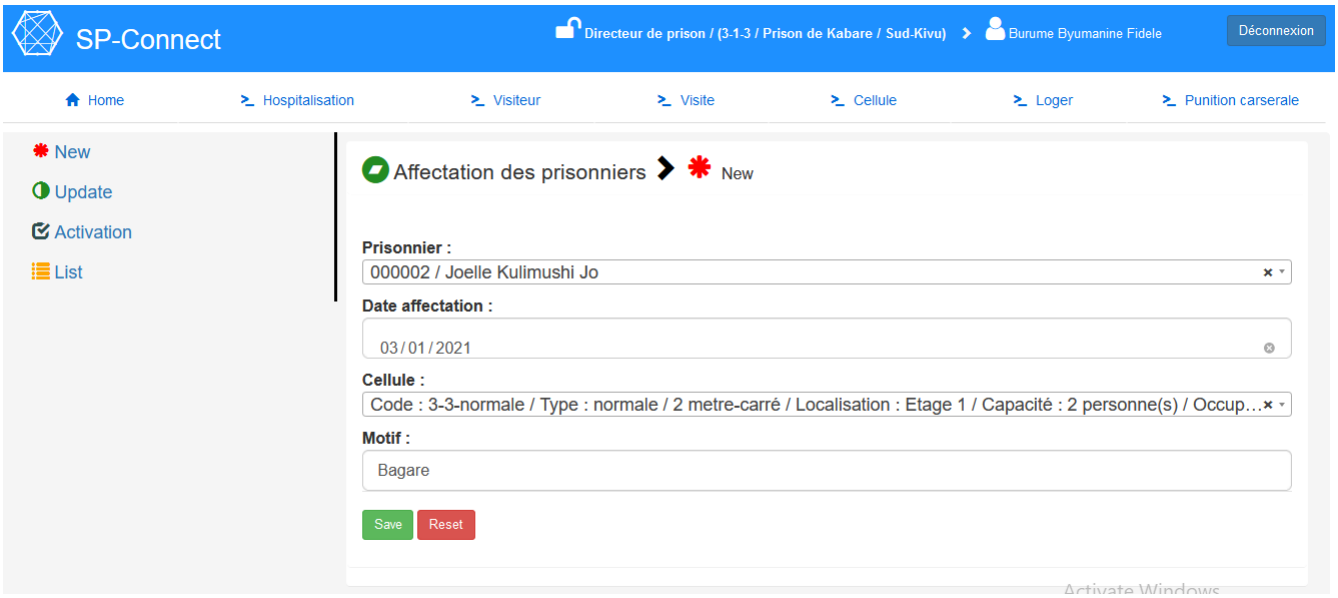


FIGURE 6.12 – Interface d'affectation des prisonniers dans les cellules

La dernière activité du Directeur de prison est l'enregistrement des mesures disciplinaires infligées contre les prisonniers. Chaque mesure disciplinaire doit faire référence à une punition. Toutes les punitions sont répertoriées et enregistrées dans le système par le ministère de la justice. La figure suivante représente l'interface d'enregistrement des mesures disciplinaires.

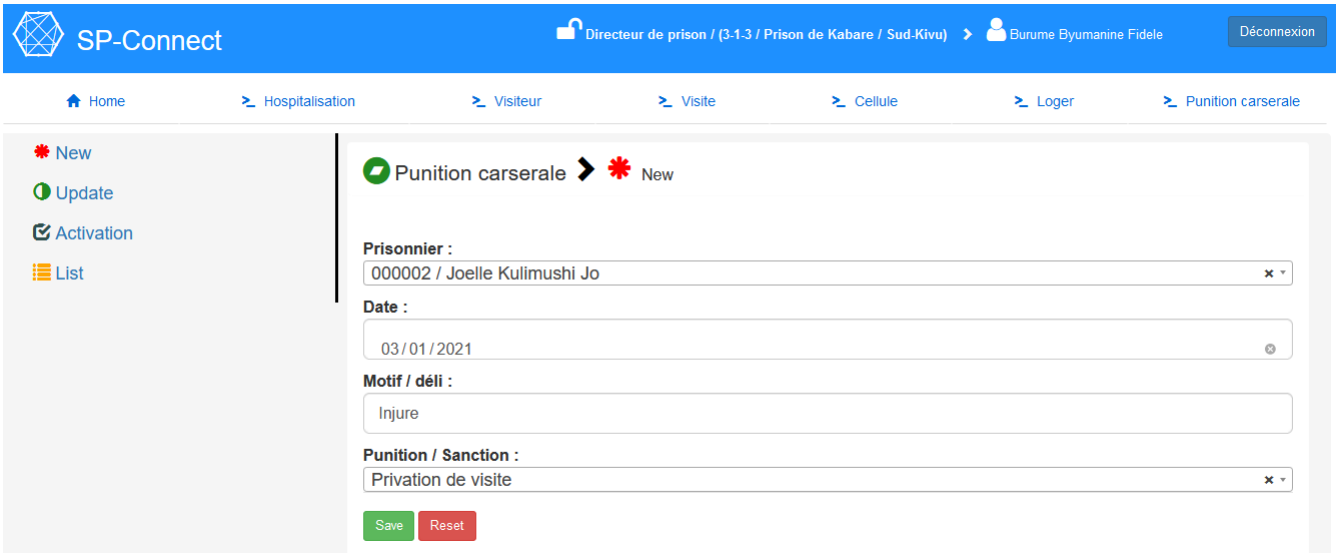


FIGURE 6.13 – Interface d'enregistrement des mesures disciplinaires

6.3.4 Administrateur du système

L'administrateur du système est chargé d'effectuer deux activités principales dans le système. Premièrement il effectue le paramétrage du système par la réalisation des configurations de base comme les informations sur les langues, les religions, les nationalités, les professions, les provinces et les types de prison. Deuxièmement, il effectue la gestion des utilisateurs et l'octroie des droits d'accès. Après s'être authentifie, l'administrateur du système accède à l'interface d'accueil

de son module. Cette interface comporte aussi menu constitué des chemins d'accès des différentes fonctionnalités. La figure suivante représente l'interface d'accueil de l'administrateur du système.

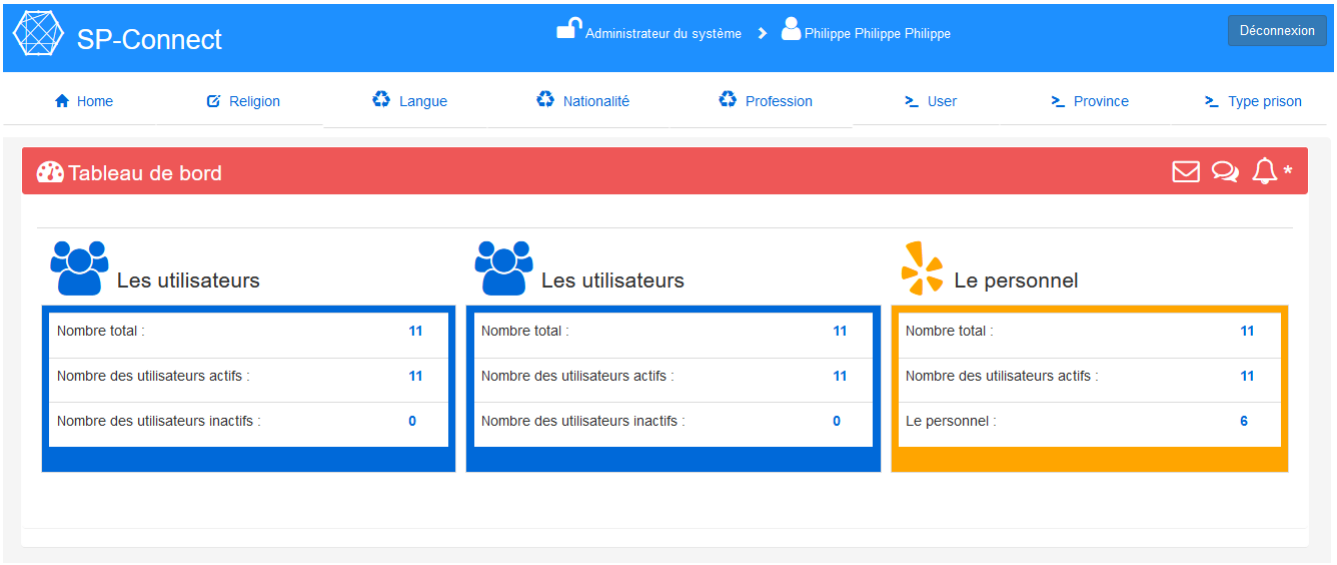


FIGURE 6.14 – Interface d'accueil de l'administrateur du système

6.4 Génération des rapports

Nous avions généré les rapports suivants :

6.4.1 Billet de sortie

Il se présente de la manière suivante :



REPUBLIQUE DEMOCRATIQUE DU CONGO
MINISTERE DE LA JUSTICE ET DROITS HUMAINS
ADMINISTRATION PENITENTIAIRE
Province du(de) Sud-Kivu
Prison de Kabare

FICHE DE LIBERATION

Le(La) nommé(e) Buhendwa Ishara Paul / Sexe :M
N° : 003..... N° RMP : 000 ..... N° RP : 000
Arrêté(e) le : 02/02/2021 / Par : 02211 / Balola Bigirimana Romain
Poursuivi(e): du chef de : 1.Viol,
Condamné(e) a : 269 mois De SPP 0 mois de SPS et de 0 mois de CPP
Est libéré(e) ce jour par : Balola Bigirimana Romain DEP SPP

Fait à Bukavu le 02/03/2021
Le directeur de (de la, du) Prison de Kabare

Burume Byumanine Fidele

FIGURE 6.15 – Billet de sortie

Le billet de sortie est constitué des détails concernant la libération du prisonnier. Il est imprimé par le greffier après enregistrement de la libération. Le bouton "sortie" du menu principale du greffier permet d'accéder à l'interface d'enregistrement des sorties. Les libérations enregistrées sont présentées dans une liste accessible par un clic sur le bouton "liste" du menu secondaire. Cette liste comporte un bouton, pour chaque item, pouvant permettre de lancer l'impression d'un billet de sortie y associé. Seul le Directeur de prison a le droit d'imprimer le billet de sortie d'un prisonnier. La figure ci-dessous représente l'interface d'impression des billets de sortie.



FIGURE 6.16 – Interface-billet-de-sortie

6.4.2 Fiche d'identification d'un détenu

Elle se présente de la manière suivante :

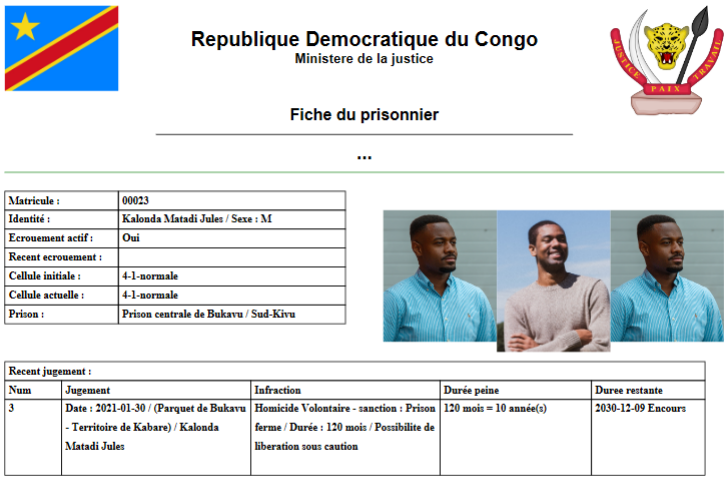


FIGURE 6.17 – Fiche d'identification d'un détenu

Après enregistrement des informations administratives d'un détenu, son ecrouement et les peines prononcées ; le greffier pourra alors imprimer la fiche d'identification du détenu en question.

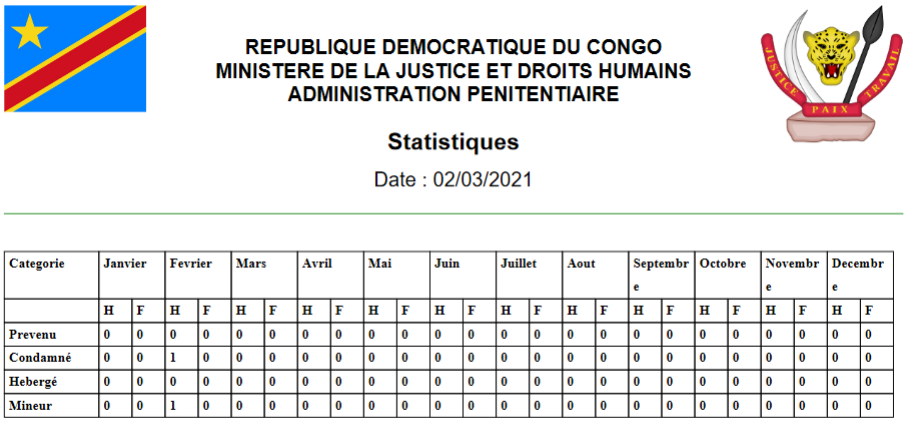
Cette fiche comporte aussi trois photos d'identifications du détenu correspondant aux trois vues d'observation (vue de face, vue de gauche et vue de droite). Le bouton d'impression de cette fiche est accessible sur le résultat obtenu lors de la recherche d'un prisonnier directement sur l'interface d'accueil. Voir la figure ci-dessous.



FIGURE 6.18 – Interface d'impression de la fiche d'identification d'un détenu

6.4.3 Statistiques par prison

Elle se présente de la manière suivante :



REPUBLIQUE DEMOCRATIQUE DU CONGO
MINISTERE DE LA JUSTICE ET DROITS HUMAINS
ADMINISTRATION PENITENTIAIRE

Statistiques

Date : 02/03/2021

Categorie	Janvier		Fevrier		Mars		Avril		Mai		Juin		Juillet		Aout		Septembre		Octobre		Novembre		Decembre	
	H	F	H	F	H	F	H	F	H	F	H	F	H	F	H	F	H	F	H	F	H	F	H	F
Prevenu	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Condamné	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hebergé	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mineur	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

FIGURE 6.19 – Fiche des statistiques par prison

Le Directeur de prison, le greffier et l'agent du Ministère de la justice peuvent tous imprimer cette fiche. Particulièrement pour le Ministère de la justice, cette fiche englobe les statistiques des toutes les prisons. Pour chaque utilisateur précité, le bouton d'impression est directement accessible sur le tableau de bord. La figure ci-dessous représente le tableau de bord contenant le bouton d'impression de la fiche des statistiques.

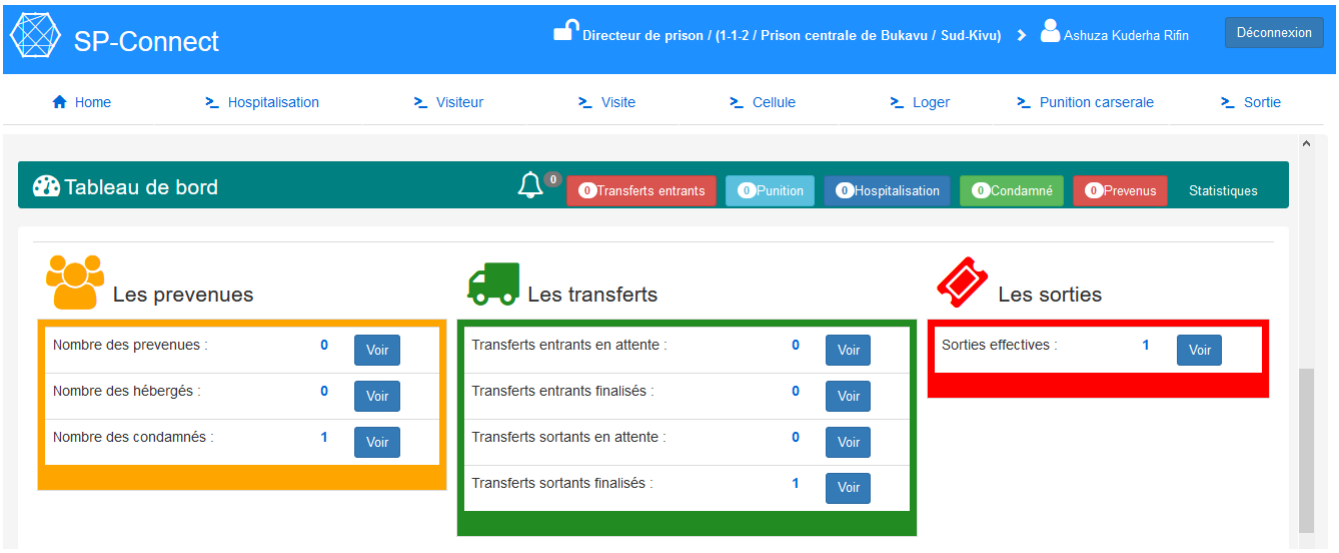
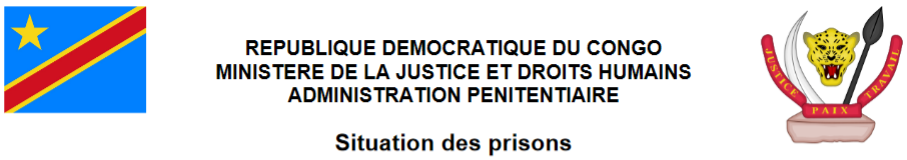


FIGURE 6.20 – Interface d'impression des statistiques

6.4.4 Population pénitentiaire globale

La fiche de la situation des prisons est un état de sortie important permettant au Ministère de la justice d'avoir une vue globale de la population carcérale dans toutes les prisons. Le dénombrement pour chaque prison est réalisé sur base du genre des prisonniers incarcérés. Cette fiche se présente de la manière suivante :



REPUBLIQUE DEMOCRATIQUE DU CONGO
MINISTERE DE LA JUSTICE ET DROITS HUMAINS
ADMINISTRATION PENITENTIAIRE

Situation des prisons

Date : 03/03/2021

Categories	Prevenu		Condamné		Hebergé		Mineur		Total	
	H	F	H	F	H	F	H	F	H	F
Prison centrale de Bukavu	0	0	1	0	0	0	1	0	1	0
Cachot du commissariat Ibanda	0	0	0	0	0	0	0	0	0	0
Prison de Kabare	0	0	2	1	0	0	2	0	2	1
Prison de Makala	0	0	0	0	0	0	0	0	0	0
									3	1
Grand total									4	

FIGURE 6.21 – Fiche de la population pénitentiaire globale

6.5 Résultats principaux et discussions

Cette partie permet de mettre en évidence les résultats principaux par rapport à tous les problèmes que nous avions soulevés dans le système pénitentiaire congolais.

6.5.1 Par rapport au problème d'irrégularité

Pour résoudre ce problème, nous avons mis en place un tableau de bord qui permettra de signaler automatiquement tous les cas d'irrégularités qui nécessitent une attention particulière. C'est notamment le cas de tous les prévenus ayant dépassés leurs durées d'observation, de tous les condamnés ayant dépassés leurs durées de peine, etc. Pour chaque cas d'irrégularité, le système affichera des notifications sur le tableau de bord afin de garantir une signalisation en temps réel. Cet outil se présente de la manière suivante :

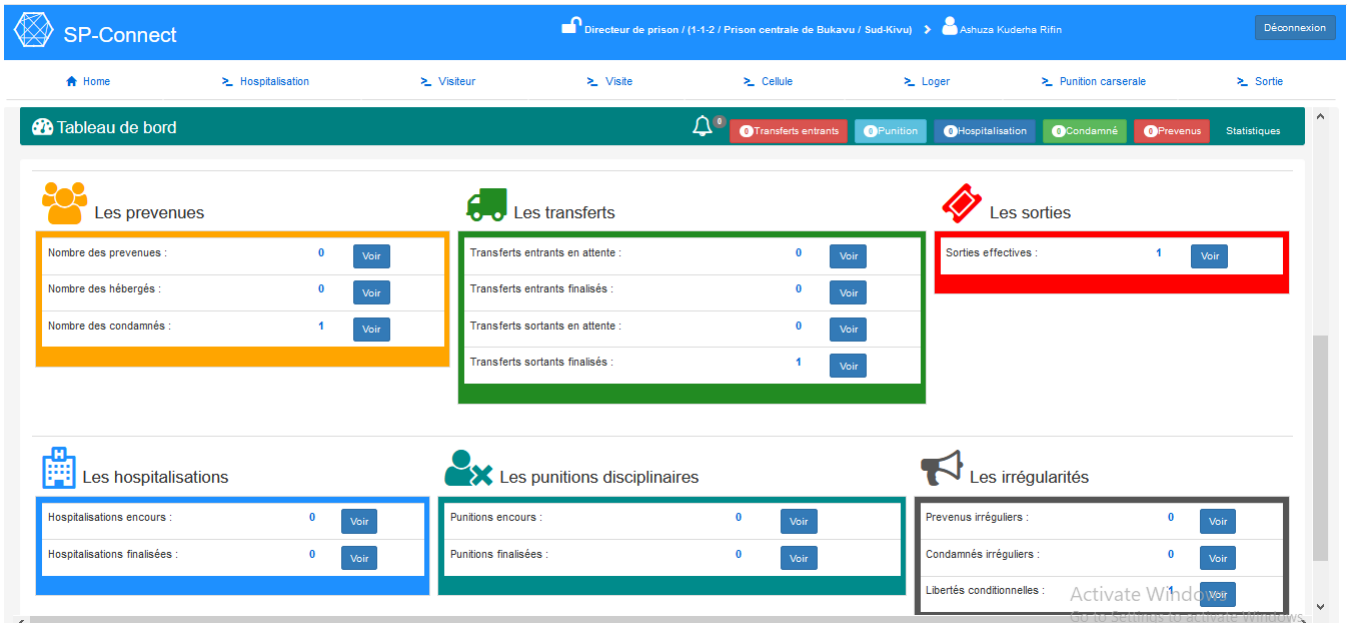


FIGURE 6.22 – Interface d'impression des statistiques

6.5.2 Par rapport au problème de la recherche d'information

Nous avions mis en place au moyen du langage SQL, un formulaire de saisie des critère et l'affichage des données remplissant ces critères. La figure suivante nous montre cela.

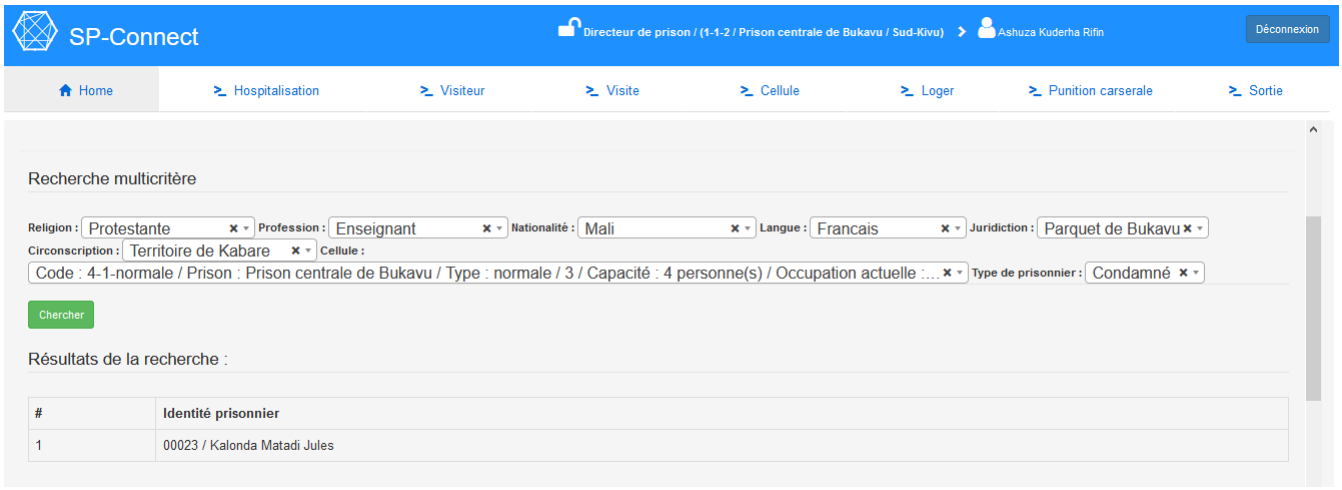


FIGURE 6.23 – Résultats de la recherche multi-critères

6.5.3 Par au problème d'accès aux données en temps réel

Par rapport au problème d'accès aux données en temps réel, nous avions conçu et réalisé un système ayant une base de données unique stockant l'ensemble d'information du système pénitentiaire sur toute l'étendue de la RDC. Le déploiement de ce système utilise une approche client serveur. Cela signifie que toutes les prisons seront considérées comme clients et le serveur pourra stocker l'ensemble des données et application. Pour permettre une utilisation efficace de ce système, entre plusieurs utilisateurs, nous avions mis sur pied deux mécanismes pour garantir la cohérence des données :

- L'affichage d'un menu adaptatif par rapport à la catégorie de l'utilisateur après une connexion réussie et
- Un filtrage des données spécifiques de la prison à laquelle appartient l'utilisateur connecté. (Ex : un utilisateur X affecté à la prison Y n'aura accès qu'au données relatives à la prison Y).

Par contre, le Ministère de la justice quant à lui aura accès à toutes les données de toutes les prisons par rapport aux décisions générales qu'il est appelé à prendre. Cette approche utilisée ici est une alternative de l'approche des bases de données reparties. Nous pensons avoir proposé un moyen efficace pour gérer un système multi-sites lorsque les données locales par site sont régulièrement utilisées localement. Le système de filtrage dont il est question ici est comparable à la fragmentation horizontale dans les bases de données réparties.

6.5.4 Par rapport à l'élaboration des rapports

Face à ce problème qui constitue une épineuse question lorsque le traitement et le stockage des données sont manuels, nous avons élaboré un algorithme en PHP qui permet de créer des rapports en si peu de temps dans un format PDF. Cet algorithme peut être utilisé pour la même finalité pour une autre tâche en adaptant les données qu'on cherche à imprimer.

6.5.5 Par rapport problème de surpopulation dans les prisons

Nous avions mis sur pied un mécanisme permettant de transférer les prisonniers d'une prison à une autre. L'idée est d'essayer d'équilibrer le nombre d'individus par prison par rapport à la capacité d'accueil. Aussi, au sein d'une même prison, les cellules déjà dépassant leurs capacités d'accueil seront facilement réparables.

6.5.6 Par rapport au problème de la non possibilité de demande de la liberté conditionnelle

Désormais avec ce système, il sera plus facile de se faire une idée sur le comportement d'un individu, gage d'une liberté conditionnelle. On pourra ainsi utiliser un contrôle sur les critères suivants : nombre de mesures disciplinaires subis, nombre de changements des cellules, nombre de transferts de prison et l'accomplissement du quart de la peine.

Cet aspect pourra toutefois être enrichi si on pouvait formaliser toutes les règles de bonne conduite en prison d'une part et d'autre part avoir une surveillance en temps réel de tout mouvement d'un détenu. On pourra ainsi élaborer un algorithme permettant de proposer une côte objective sur une échelle quelconque. Cet algorithme pourra être utilisé dans une société fortement surveillé par des cameras afin de bonifier tous les bons actes et de pénaliser tous les mauvais actes.

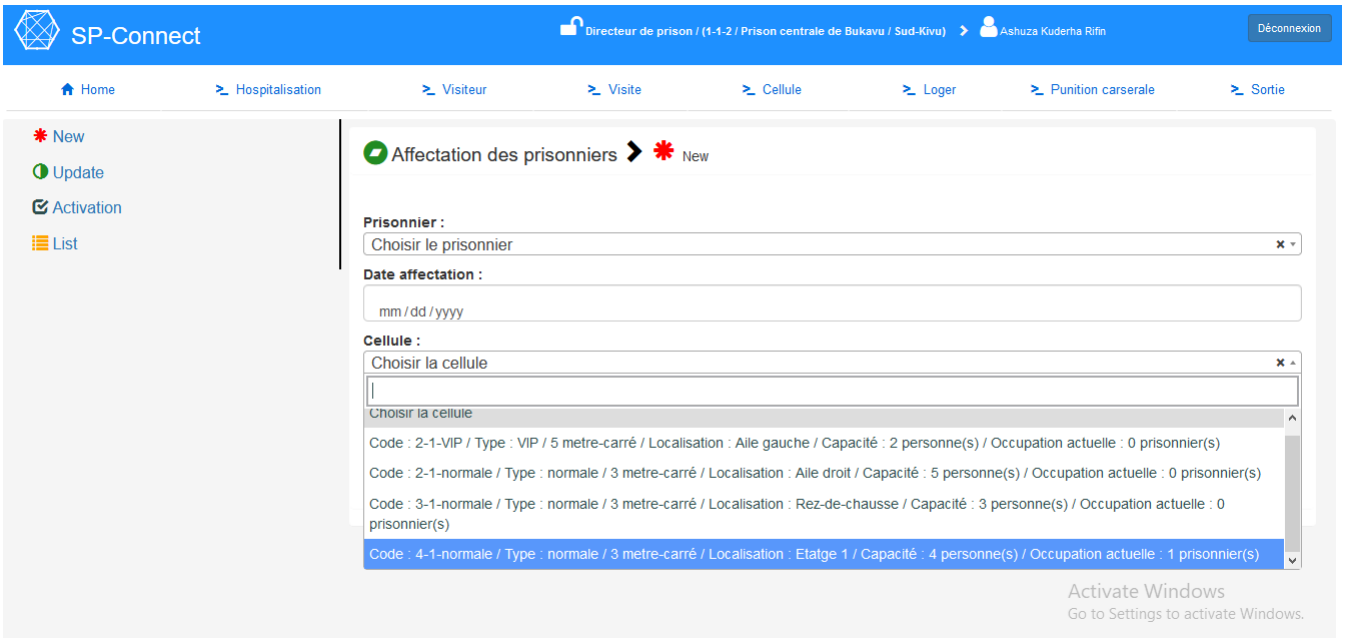


FIGURE 6.24 – Contrôle de la capacité d'accueil des cellules

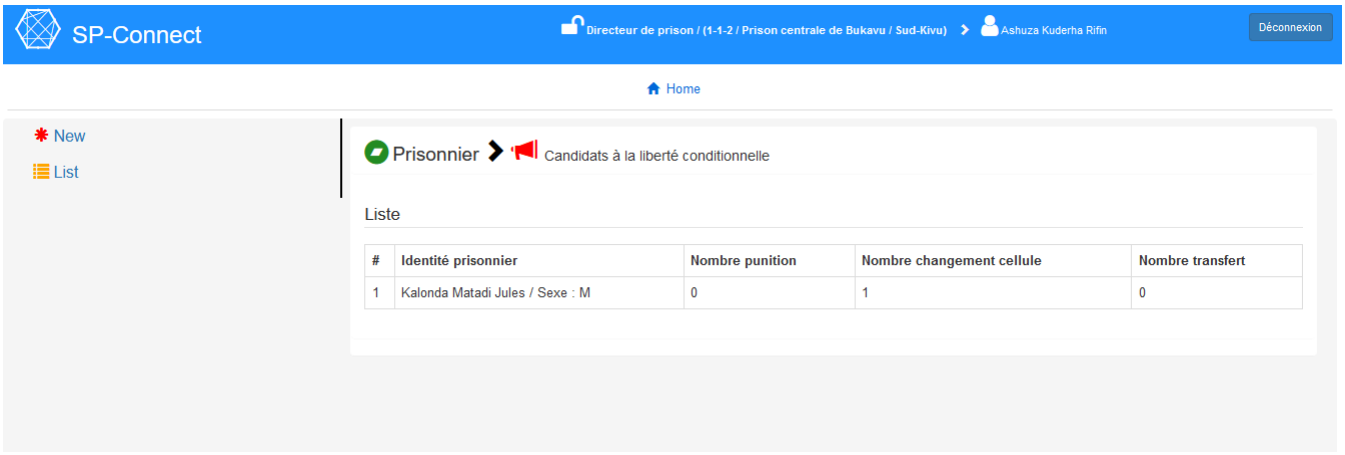


FIGURE 6.25 – Interface de visualisation des candidats à la liberté conditionnelle

6.5.7 Sécurité

Comme tout système d'hébergement en ligne, il a été utile de sécuriser ce dernier. Nous avions sécurisé notre système à partir du mot de passe fourni par l'utilisateur en le cryptant avec RSA. Nous avions ainsi réalisé un moyen de s'authentifier à un système d'une manière sure en rendant inintelligible ces informations secrètes au moment de leur transmission au serveur. Nous pensons que ce résultat peut être utilisé par n'importe quel développeur ayant le souci de sécuriser son système au moment de son accès.

6.6 Processus d'hébergement du projet SP-CONNECT

6.6.1 Introduction

La philosophie actuelle appliquée dans l'utilisation des solutions logicielles est la mise en disponibilité du système à la portée de tous les utilisateurs peu importe leur localisation géographique. Le système est alors installé dans un ordinateur auquel on peut accéder de n'importe où dans le monde, on parle alors de l'hébergement de l'application. Il fait parti d'un des services du cloud computing. L'ordinateur utilisé doit alors avoir une capacité de stockage importante et une entité de calcul assez puissante pour supporter l'exécution de toutes les requêtes lancées par les utilisateurs.
Le projet SP-Connect étant sensé être utilisé dans les structures pénitentiaires dispersées à travers le pays, il est alors nécessaire de l'héberger pour garantir l'accessibilité à celui-ci à tous les utilisateurs présents dans ces structures.

6.6.2 Présentation de la technique d'hébergement

L'hébergement d'une solution informatique fait intervenir deux concepts. Il s'agit de l'espace d'hébergement et du nom de domaine.

Espace d'hébergement : L'espace d'hébergement est constitué d'un espace de stockage de données ayant une capacité définie et d'un système de gestion de base de données (SGBD). Le rôle du premier est de stocker les fichiers constitutifs de l'application. Celui du second est de stocker la base de données de l'application.

Nom de domaine : L'ordinateur (serveur) qui héberge l'application étant connecté sur le réseau internet, il possède alors une adresse IP permettant de l'identifier sur le réseau. Le nom de domaine en soit est la traduction de l'adresse IP du serveur en url par le serveur DNS. Il est alors possible d'accéder à l'application via ce nom de domaine en tapant celui dans le navigateur web.

6.6.3 Procédure pour mettre en ligne SP-Connect

La procédure pour mettre en ligne SP-Connect a été constituée de plusieurs étapes. Il s'agit de :

Commande de l'espace (stockage et base de données) L'espace de stockage a été commandé chez l'hébergeur en choisissant une formule d'abonnement à laquelle souscrire. Nous avons choisi une formule d'abonnement offrant un espace de stockage d'une capacité de 15Go et un SGBD MySQL pour le stockage d'une base de données.

Commande du nom de domaine Pour avoir un nom de domaine accessible sur internet, il faut faire enregistrer dernier dans le registre mondial des noms de domaine (registrar).
Etant donné que le projet est, pour l'instant, à l'étape de développement, nous avons jugé bon d'utiliser un sous domaine du nom de domaine de notre hébergeur. Il s'agit de www.spconnect.aretn.cd
Nous pourrons alors commander un nom de domaine final lorsque le système sera à l'étape de production dans un environnement réel d'utilisation.

Mise en ligne du projet (fichiers) et importation de la base de données (PhpMyAdmin distant) Pour transférer le fichier du projet vers l'espace de stockage du serveur nous avons utilisé le logiciel Filezilla version 3.51.0 qui permet le transfert de fichier vers une machine distante via le protocole FTP.
L'importation de la base de données de l'application vers le SGBD MySQL du serveur a été effectuée à l'aide de l'outil PhpMyAdmin disponible dans l'espace d'administration de l'hébergement.

Test Après la mise en ligne de l'application (fichiers sources et base de données), nous avons effectué une batterie de test afin de vérifier si la procédure d'hébergement a été effectué avec succès. Il s'agissait d'accéder aux différentes fonctionnalités de l'application en tapant l'url du nom de domaine dans le navigateur sur un ordinateur connecté sur internet. Les tests effectués ont été conclus positifs.

Mises à jour La mise en ligne d'une nouvelle version du logiciel et l'application des modifications sur la base de données peuvent être effectuées via le logiciel de transfert de fichier Filezilla et l'outil PhpMyAdmin.

L'hébergement d'une solution informatique sensée être partagé entre plusieurs utilisateurs résidant dans des régions géographiques séparées s'avèrent être une bonne approche pour garantir l'accessibilité et la disponibilité des fonctionnalités et des données.
Le système SP-Connect étant appelé à fonctionner dans un contexte similaire, son hébergement sur un serveur distant a été une nécessité incontournable.
Certes, l'hébergement nécessite des coûts financiers mais les avantages offerts par celui-ci sont nombreux.

6.7 Coût du logiciel

6.7.1 Méthode COnstructive COst MOdeL

La méthode COCOMO a été développé par Dr. Barry Boehm pour estimer l'effort et le temps de développement d'un produit logiciel.[28][30]
On retrouve trois types de projets logiciels :
- Organique : <50KLOC
- Semi détaché : <300KLOC
- Imbriqué : >300KLOC

Table 6.1 – Valeurs paramètres COCOMO

Types de projet	Effort	Productivité
Organique	$HM = 2.4 * (KLOC)^{1.05}$	$TDEV = 2.5 * (HM)^{0.38}$
Semi-détaché	$HM = 3 * (KLOC)^{1.12}$	$TDEV = 2.5 * (HM)^{0.35}$
Imbriqué	$HM = 3.6 * (KLOC)^{1.2}$	$TDEV = 2.5 * (HM)^{0.32}$

6.7.2 Méthode COCOMO II

La méthode COCOMO II a été mis sur pied pour améliorer le calcul fait par COCOMO en prenant en compte la reutilisabilité du code, en plus d'autres facteurs environnementaux.[28]

6.7.3 Méthode WebMo

La méthode WebMo est la méthode COCOMO II adaptée aux projets web.Elle fut conçue par Reifer sous le nom de WebMo. Ce nouveau modèle diffère de COCOMO II par l'introduction d'une nouvelle métrique de mesure de la taille appelée Objets Web (Web Objects) et par une re-calibration des paramètres de COCOMO II.[29]
Le nombre de multiplicateurs est passé de 17 à 9.

L'équation de base de WebMo pour l'effort est alors la suivante :

$$Effort = A * (Taille)^{P_1} * \prod_{i=1}^{9} EM_i \tag{6.1}$$

La constante A et l'exposant d'échelle Pl varient selon le domaine d'application,comme présenté dans le tableau 6.2.

Table 6.2 – Valeurs paramètres WebMo

Domaine d'application	A	P1
Commerce électronique	2.3	1.03
Applications commerciales et financières	2.7	1.05
Applications Business-to-Business	2.0	1.00
Portails web	2.1	1.00
Utilitaires d'informations web	2.1	1.00

6.7.4 Calcul du Coût de notre projet avec WebMo

Nous allons calculer le cout du projet avec la méthode webMo, étant donné que notre application est web. Nous allons utiliser les paramètres de la catégorie "Portails web". Le nombre des lignes codes de notre application vaut :10234

$$Taille = 10.234$$
$$A = 2.1$$
$$P1 = 1.00$$
$$\prod_{i=1}^{9} EM_i = 1$$
$$Effort = 10.234 * 2.1 = 21.5HM$$
$$TDEV = 2.5 * (21,5)^{0.38} = 8Mois$$
$$Productivit = 10234/21.5 = 476lignesdecodes$$
$$Tailleequipe = 21.5/8 = 2,6$$

Interprétation : 21,5HM signifie que ce projet exigerait soit 21,5 mois s'il devait être exécuté par une seule personne ou soit 21,5 personnes pour le réaliser dans un mois.
Mais en réalité, nous l'avions réalisé en 10 mois comme présenté par le diagramme de Gantt au premier chapitre, ce qui signifierait peut être que le travail de 21,5 mois a été réalisé en 10 mois. Cela peut s'expliquer car ce projet est réalisé dans un cadre de travail de fin d'étude, où la contrainte sur une certaine durée de sa réalisation était de rigueur. Quant au Coût financier de ce projet, il suffirait de fixer un montant forfaitaire par mois, en tenant compte de la réalité de l'environnement. Ainsi, par exemple si on doit être payé 500 dollars le mois, on aura :

$$Coutfinancier = 500 * 21.5 = 10750 dollars$$

6.8 Conclusion au chapitre sur la présentation de l'application

Dans chapitre, nous explorons les fonctionnalités du produit informatique réalisé tout en insistant sur les principaux résultats obtenus et les rapports générés par ce dernier. Ce chapitre est clos par une petite littérature sur ce qu'on doit savoir sur son coût financier ainsi que l'hébergement d'une application en ligne, un moyen que nous avions utilisé pour déployer matériellement et physiquement la présente application.

CONCLUSION

Depuis l'invention de la roue, l'homme cherche à optimiser sa manière de travailler en automatisant ses tâches. Actuellement la plupart d'entreprises et sociétés font usage des NTIC dans la réalisation de leurs activités en vue d'améliorer leurs services et accroître ainsi leur rentabilité. Malheureusement les prisons en RDC, adoptent encore une approche manuelle, qui est non efficace par rapport aux objectifs qui leur sont assignés.

En effet, les difficultés liées aux traitements manuels des différentes tâches engendrent non seulement une perte de temps dans l'exécution des tâches, un abandon progressif de certaines tâches, une élaboration des rapports non en temps réel, un encombrement des visiteurs mais aussi du non respect des droits de l'homme, de l'injustice, et de la corruption.

L'objectif global a été de concevoir une application informatique et sécurisée qui exécute certains processus métiers répétitifs du système pénitentiaire jadis exécuté manuellement par l'homme. Ainsi, nous avions réalisé un module de signalisation des détenus à libérer, de recherche d'information dans une large base des données, de génération automatique des rapports, d'aide à la prise des décisions en rapport avec la politique d'amnistie, de la liberté conditionnelle et de l'octroie de casier judiciaire. Tous ces modules utiliseront une base des données unique stockant les données de toutes les prisons de la RDC et dont l'accès est sécurisé par le cryptosystème RSA.

Signalons que la stratégie que nous avions utilisée pour filtrer les informations spécifiques à chaque prison au moment de la connexion au système, peut être utilisée par n'importe quelle entreprise multi-sites dont les opérations régulières exigent des données locales. Par contre, lorsque les données de tous les sites sont sollicitées pour l'écriture et lecture simultanément, cette stratégie peut se révéler non efficace, comme c'est le cas des Banques par exemple. C'est grâce à la méthodologie UP basée sur le langage UML que le présent système a été réalisé.

Avec les solutions présentées ci-haut, nous espérons mettre fin à la détention illégale liée au dépassement de la durée de peine, la principale cause de la surpopulation des maisons carcérales ; à l'amélioration des services, à la disponibilité en temps réel des informations recherchées au sein des prisons et au suivi facilité pour chaque cas de détention et à la restauration de la justice dans les arrestations et détentions illégales sur toute l'étendue de la RDC. Ne dit-on pas que la justice élève une nation ?

RECOMMANDATIONS

Aux futurs Chercheurs :

1. Ajouter un module de vidéo-surveillance ;
2. Ajouter un module de surveillance à distance à partir d'une puce électronique incorporée dans le prisonnier ;
3. Concevoir un système embarqué qui comprend les deux modules précédents ;
4. Ajouter un module de la gestion d'empreinte digitale pour chaque prisonnier.
5. Ajouter un module de clustering pour la segmentation des données ;
6. Ajouter un module de reconnaissance faciale ;

Signalons tout de même que la plupart de ces limites ont été causées dans cette présente étude par l' indisponibilité de certains matériels technologiques et le défaut des moyens financiers pour leur acquisition.

A l'État Congolais :

1. Mettre en place ce nouveau système avec un autre centre de réplication des données ;
2. Prévoir la mise à niveau des agents de la prison par rapport à l'utilisation du nouveau système ;
3. Déployer et exploiter ce nouveau système en munissant chaque prison,maison d'arrêt, cachot d'au moins trois ordinateurs avec connexion internet et une source d'énergie efficace ;
4. Ajouter un code dans le système pénitentiaire congolais qui dit :"Nul ne peut être détenu dans une prison,maison d'arrêt et cachot s'il n'a pas été préalablement enregistré dans le présent système informatique".

Bibliographie

[1] Dabissi David LANKOANDE. Du respect des droits de l'homme en prison. Cas de la RDC. Master thesis, Université de Nantes, 2015.

[2] Monuc, Rapport sur la detention dans les prisons et cachots de la rdc, Avril 2004. www.refworld.org/pdfid/46caab0f0.pdf,consulté le 02/07/2020.

[3] Monuc, Arrestation et détention dans les prisons et cachot de la RDC, mars 2006

[4] Monuc, Rapport sur les conditions de détention dans les prisons et cachots de la RDC,2005.

[5] Ministère de la justice Ordonnance 344 du 17 septembre 1965 relatif au régime pénitentiaire de la République Démocratique du Congo,1965.

[6] Ministère de la justice, Le Code de procédure pénale de la RDC, Décret du 6 août 1959, tel que modifié et complété par la loi n 06/019 du 20 juillet 2006, 2006.

[7] Ministère de la justice, Rapport sur les statistiques pénitentiaires Juillet 2014 –Juillet 2015, 2015.

[8] Pascal Roques. UML2 Par la Pratique Etude des cas et exercices corrigées. EY- ROLLES, 2006.

[9] Benoît Charoux and all , UML2.0 , Pearson, 2008.

[10] Muller Pierre-Alain & Gaertner ,Modélisation objet avec UML, Eyrolles, 2000.

[11] Jérémie Guiochet, Le Processus Unifié Dermarche orientée modèle,2009, https ://homepages.laas.fr/guiochet/telecharge/Guiochet-SupportCoursProcessusUnifie.pdf, consulté le 12/12/2020.

[12] Elisabetta De Maria, Cours de Base de Données Cours n.3 Algèbre relationnelle,Université de Nice Sophia Antipolis.

[13] Stéphane Crozat, Algèbre relationnelle,2018 https ://www.i3s.unice.fr/ edemaria/cours/c3.pdf https ://stph.scenari-community.org/bdd/alg1.pdf, consulté le 01/12/2020.

[14] Anca Nitulescu ,Cryptosystème RSA, Ecole Normale Supérieure, Paris, https ://www.di.ens.fr/ nitulesc/files/crypto3.pdf, consulté le 05/03/2021

[15] David Pointcheval, La Cryptographie Asymétriqueet les Preuves de Sécurité,2002, https ://www.di.ens.fr/david.pointcheval/Documents/Slides/s2002_cachan.pdf,consulté 02/03/2021.

[16] Dumas Jean-Pierre,Cours UML, UFTI – IUFM Toulouse, 1998.

[17] https ://security.stackexchange.com/questions/32050/what-specific-padding-weakness-does-oaep-address-in-rsa, consulté le 01/04/2021.

[18] Ndayisaba Longin, Cours de sécurité des réseaux,Université du Burundi,2020.

[19] Douglas R., Cryptography :Theory and Pratice, 2nd ed.,CRC Press, Inc., 2002.

[20] William Stallings, Cryptograpy and Network Security,Principes and Pratice, 3e edition, Prentice Hall,2003.

[21] C.Llorens,L.Levier, Tableaux de bord de la sécurité réseau,deuxième édition, Eyrolles, 2006.

[22] Didier Muller, Les Codes secrets décryptés, City Editions, 2007.

[23] Renaud Dumont, Notes de cours sur Cryptographie et sécurité informatique, Université de Liège, 2010.

[24] Matthieu Exbrayat, Bases de données réparties, 2009.

[25] Dave Odilon, Bases de données réparties sous oracle, Ecole supérieur de management commerce et informatique, http ://www.memoireonline.com/05/10/3459/mbases-de-donnees-reparties-sous-oracle.html, consulté le 06/11/2020.

[26] Philippe Rigaux, Cours de bases de données, 2001.

[27] Philippe Rigaux, Evaluation et optimisation des requêtes, http ://sys.bdpedia.fr/optim.html, consulté le 10/12/2020.

[28] http ://users.polytech.unice.fr/ hugues/GL/chapitre3.pdf, consulté le 02/05/2021.

[29] Oualid Ktata, estimation de projets web : application et analyse de fiabilité des modèles cocomo ii et webmo, https ://archipel.uqam.ca/3264/1/M9720.pdf, consulté le 02/05/2021.

[30] https ://www.estimancy.com/fr/2018/03/27/le-mode-cocomo/, consulté le 02/05/2021.