République Algérienne Démocratique et Populaire Ministére de l'Enseignement
Supérieur et de la Recherche Scientifique

MÉMOIRE DE FIN D'ÉTUDE

MASTER PROFESSIONEL
Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique
Option Administration et Sécurité des Réseaux

Thème

Conception et réalisation d'un système de messagerie sécurisé

Réalisé par : SEMCHAOUI Sabrina

Devant le jury composé de :

- Président : M^r AISSANI Sofiane MCA Université de Béjaia
- Examinatrice : M^{me} HOUHA Amel MAA Université de Béjaia
- Encadreur : M^{me} SABRI Salima MCB Université de Béjaia

Promotion 2019/2020

$\mathcal{R}$emerciements

Je tiens tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui m'a donné la force et la patience d'accomplir ce modeste travail. Mes fort et sincère remerciements à mon encadreur madame SABRI Salima pour ses précieux conseils et ses orientations ficelées tout au long de mon projet.

Mes vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à mon travail en acceptant de l'examiner et de l'enrichir par leurs propositions. Enfin, Je tiens également à remercie toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Dédicaces

À
mes parents
mes deux soeurs
mon frére
tous membres
de ma famille
tous mes amis

Sabrina.

Table des matières

Table des figures

Liste des tableaux

Notations et symboles

ARPANET	Advanced Research Projects Agency Network
BDD	bases de données
DoD	Department of Defense
GPG	GNU Privacy Guard
IMAP	Interactive Mail Access Protocol
MDA	Mail Delivery Agent
MIT	Massachusetts Institute of Technology
MSA	Mail Storage Area
MSS	Mail Storage Server
MTA	Mail Transfert Agent
MUA	Mail User Agent
POP3	Post Office Protocol version 3
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
UML	Unified Modeling Language
YUI	Yahoo User Interface

Introduction générale

Aujourd'hui, le monde connaît une avancée considérable dans l'utilisation des applications web et mobiles, ces dernières sont capables de satisfaire les besoins actuels des utilisateurs avec de nombreuses fonctionnalités et en offrant plusieurs services comme le service de communication.

La communication n'a pas cessé de se développer, devenant ainsi de plus en plus technique. Il s'agit d'une notion moderne, qui n'a fait qu'évoluer jusqu'à devenir aujourd'hui un élément fondamental de la stratégie d'entreprise. La messagerie permet entre les personnes une communication asynchrone bénéficiant de la précision de l'écrit et de la souplesse du langage naturel. Actuellement, les services de messagerie sont beaucoup plus riches et présentent beaucoup plus de fonctionnalités ; à savoir l'intégration des pièces jointes (joindre un fichier quelconque au message envoyé), la gestion du courrier indésirable (les spams) et la manipulation des listes de diffusion (l'envoi multiple). Notre projet s'inscrit dans un cadre général du développement et de la réalisation d'un «Système de messagerie sécurisée sur une plateforme web » qui permet à plusieurs utilisateurs d'échanger des messages et les sauvegarder dans une base de données et les sécuriser. Notre mémoire est structuré en trois chapitres. Le premier chapitre porte sur le système de messagerie et ses composants, illustré sous forme d'une architecture où nous présentons les diverses fonctionnalités de la messagerie ainsi que les différents protocoles qui le régissent.

Le deuxième chapitre sera consacré à la conception qui est une étude préalable du projet, elle est une étape primordiale et un passage obligatoire, car il s'agit de décrire les besoins de système, nous mondélisons avec le langage UML.

La réalisation de l'application fera l'objet du chapitre trois, ou nous avons présenté les outils ainsi que les langages de programmations utilisés, nous allons expliquer le fonctionnement de notre application via quelques interfaces et un scénario. nous conclurons ce mémoire par exposer l'ensemble des connaissances acquises au cours de la réalisation du projet, et exposer quelques perspectives.

Chapitre 1

ETUDE PRELIMINAIRE

1.1 Introduction

La messagerie électronique est l'une des applications d'Internet les plus anciennes, la première messagerie (Le courrier électronique) est une méthode par laquelle un message numérique est délivré d'un expéditeur à un ou plusieurs destinataires. L'histoire du courrier électronique a commencé au Massachusetts Institute of Technology (MIT) en 1965 sous le nom de Mail Box, dans le but d'envoyer des fichiers d'un ordinateur à un autre. Une percée majeure a été observée en 1971 avec l'apparition d'un véritable système de messagerie, lorsque Ray Tomilson, qui travaillait pour le ministère de la Défense (DoD), s'est envoyé son premier e-mail ARPANET [1] [13].

Dans ce chapitre nous parlons de la messagerie électronique, son fonctionnement, architecture, environnement typique, ainsi sur les protocoles de la messagerie et les protocoles de sécurité.

1. ARPANET : Premier réseau à transfert de paquets développé aux États-Unis

1.2 Notions liées à l'application messagerie web

1.2.1 Messagerie

Un service de messagerie, dans sa forme la plus basique, est un service permettant essentiellement l'échange de messages textuels entre les différents utilisateurs enregistrés (ayant une adresse électronique valide) et connectés à un réseau informatique, que ce soit en local ou sur internet . Cet échange de messages peut s'effectuer en différé, c'est-à-dire il n'est pas nécessaire que le destinataire soit connecté au moment de l'envoi, son message sera enregistré sur un serveur et il pourra le consulter ultérieurement [15].

1.2.2 Composants d'un système de messagerie

Le service de messagerie est constitué de trois entités distinctes qui coopèrent et communiquent par le biais de protocoles bien défini afin d'assurer un service entre utilisateurs.

- **MUA (Mail User Agent)** : c'est le client de messagerie, c'est un programme qui permet de lire et écrire les messages. Il formate les messages en partance afin de les donner au MTA, et les messages de la boîte aux lettres afin de les afficher à l'écran [12].

- **MTA (Mail Transfert Agent)** : lors de l'envoi, l'e-mail est envoyé vers un premier serveur de messagerie appelé : MTA ou serveur de messagerie sortant. Son rôle est d'établir en fonction du nom domaine contenu dans l'adresse mail du destinataire quel est le serveur chargé de le prendre en charge. Il lui envoie alors l'e-mail. Le protocole de communication utilisé est le SMTP (Simple mail Transfer Protocol) [12].

- **MDA (Mail Delivery Agent)** : ce serveur est aussi appelé Serveur de courrier entrant, les MDA servent à récupérer le courrier électronique. Ils

distribuent le courrier dans les boîtes des utilisateurs spécifiés [17].

- **MSA (Mail Storage Area ou surface de stockage des courriers)** : Système ou serveur local dans lequel le programme MTA stocke du courrier électronique. Il s'agit également de l'emplacement à partir duquel le serveur MSS extrait du courrier électronique à la demande de l'application MUA [12].

- **MSS (Mail Storage Server)** : Programme permettant d'extraire du courrier électronique de la zone MSA en utilisant IMAP et POP3 et de le renvoyer à l'application MUA [12].

1.2.3 Fonctionnement d'un système de messagerie électronique

Le fonctionnement d'un système de messagerie est illustré par la figure suivante :

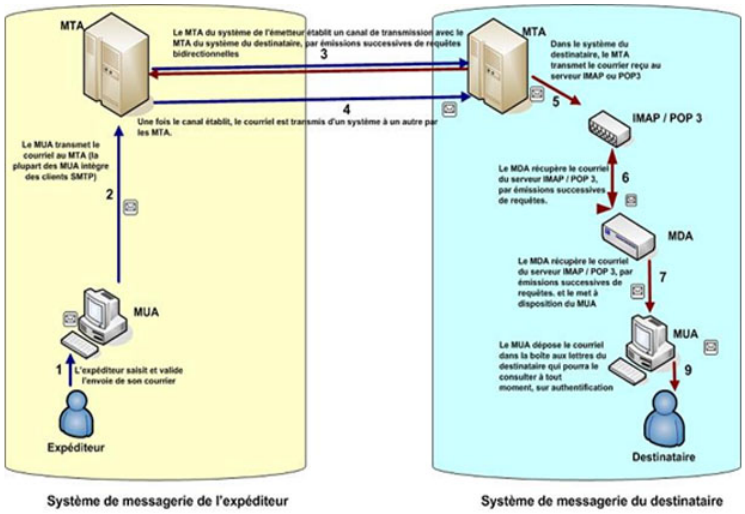


FIGURE 1.1 – le fonctionnement de la messagerie [14]

Le courrier électronique est transmis via les composants du serveur de messagerie comme suit :

1. Dans son application MUA, l'expéditeur crée un courrier électronique et clique sur Envoyer ;
2. Le programme MUA utilise SMTP pour envoyer le courrier électronique à un agent MTA ;
3. L'agent MTA relaie et achemine le courrier électronique vers un MTA dans le domaine du destinataire ;
4. L'agent MTA du domaine du destinataire envoie le courrier électronique à un MDA du système du destinataire ;
5. Le MDA stocke le courrier électronique dans une zone MSA ;
6. Le programme MUA du destinataire interroge un MSS ;
7. Le MSS utilise IMAP ou POP pour extraire le courrier électronique pour le destinataire à partir de la zone MSA ;
8. Le MSS renvoie le courrier électronique à l'application MUA ;
9. Dans son programme MUA, le destinataire lit le courrier électronique envoyé par l'expéditeur. [4]

1.2.4 Environement de messagerie Typique

on distingue 2 protocoles :

- Les protocoles de récupération de messages : POP ou IMAP
- Le protocole de transfert de messages :SMTP

[5]

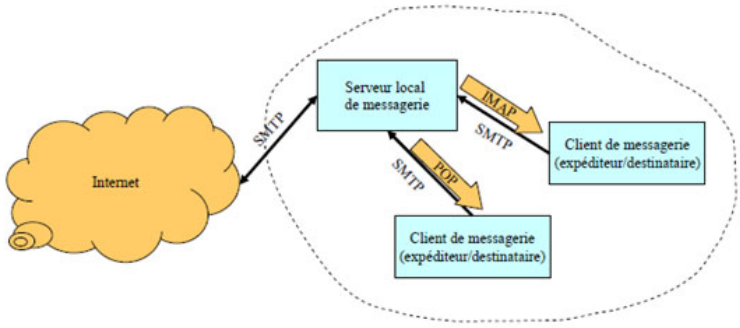


FIGURE 1.2 – Environnement de la messagerie [18]

1.2.5 Architecture de base d'un système de messagerie

La messagerie se compose de :

- Clients de messagerie : (graphiques) Eudora, Outlook, (commandes) mail.
- Serveurs de messagerie : Sendmail (le plus courant), postfix, Qmail.

1.2.6 Caractéristique d'un système de messagerie

Les principaux atouts d'une messagerie sur le web sont les suivants [10] :

- **L'asynchronisme :**
  - Possibilité d'envoyer un message même si le destinataire n'est pas connecté
  - Consultation d'un message au moment choisi
- **L'abolition des distances :** comme sur Internet en général
- **Interopérabilité :** c'est la capacité technique que plusieurs systèmes puissent opérer ensemble sans aucun conflit et sans aucune ambiguïté
- **La communication de groupe :**
  - Possibilité de "mailing" (envoi groupé), de listes de diffusion personnelles
  - Courrier électronique à la base des listes de discussion, des forums
- **La trace écrite des messages :**
  - La conservation, l'archivage des messages
  - L'exploitation des données

  - Le classement des messages
- **L'envoi de documents joints :** ces pièces jointes peuvent être des photos des document
- **La réutilisation des messages :**
  - Transférer, répondre .

Les inconvénients de la messagerie sont les suivants [10] :

- **Confidentialité des messages réduite (mais protégée par la loi) :** un message électronique est comme une carte postale envoyée sans enveloppe, visible par les facteurs...etc.
- **Propagation des virus :** le courrier électronique est le premier et principal vecteur de propagation des virus informatiques.
- **Messages abusifs, le spam.**
- **Rumeurs (hoax) :** désigne une fausse information circulant sur internet. Dans la plupart des cas, il s'agit d'un canular ou d'une rumeur. Les réseaux sociaux et le courrier électronique sont les principaux vecteurs de diffusion d'un Hoax.
- **Le "Déluge informationnel", la surinformation :** expérience quotidienne des personnes ayant une grande utilisation de leur messagerie et "croulant" sous les dizaines ou les centaines de messages quotidiens à trier...[5]

1.3 Serveur de messagerie

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour objectif de transférer des messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie, soit une interface web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages [19].

1.3.1 Protocoles de messagerie électronique

Les principaux protocoles utilisés par un serveur de messagerie sont les suivants [7, 9] :

1.3.1.1 SMTP (Simple Mail Transfer Protocol)

SMTP est un protocole de niveau application, orienté connexion. Est le protocole standard permettant de transférer le courrier entre deux serveurs de messagerie : celui de l'expéditeur et celui du destinataire. Il spécifie aussi l'entête des courriers (from ; to ; etc...), les possibilités d'envoi groupé, la gestion des heures ou encore le format des adresses des utilisateurs.

Le client SMTP doit :

- Assurer la conservation du message, tant qu'il n'est pas totalement délivré au serveur ;
- Notifier le résultat de l'expédition du message à l'expéditeur ;
- Ajouter des informations de trace dans l'entête du message

1.3.1.2 POP3 (Post Office Protocol version 3)

POP est un protocole standard Internet de couche application, Utilise le protocole TCP (port 110), il est Sous forme de Commande/réponse. Il permet d'aller récupérer son courrier sur un serveur distant (le serveur POP) aussi de créer une seule boîte aux lettres sur le serveur. Ce protocole est nécessaire pour les personnes qui ne sont pas connectées en permanence à l'Internet messagerie autrement dit POP prend en charge l'accès hors ligne aux messages. Mais ce protocole n'est, en revanche, pas sécurisé.

1.3.1.3 IMAP (Interactive Mail Access Protocol)

Il partage de nombreuses fonctionnalités similaires avec POP3, c'est un protocole qu'un client de messagerie peut utiliser pour télécharger des courriels à partir d'un serveur de messagerie. Cependant, IMAP comprend beaucoup plus de fonctionnalités

que POP3. Le protocole IMAP est conçu pour permettre aux utilisateurs de conserver leur courrier électronique sur le serveur. IMAP nécessite plus d'espace disque sur le serveur et plus de ressources CPU que POP3, car tous les e-mails sont stockés sur le serveur.

1.3.2 Protocoles de sécurité et certification

Les protocoles et certificats les plus utilisés dans le service ou système de messagerie électronique sont :

1.3.2.1 Protocol SSL (Secure Socket Layer) TLS (Transport Layer Security)

Sont des protocoles de cryptage qui garantissent pleinement la sécurité des communications pour toutes les données échangées. Ces systèmes sont largement utilisés pour garantir la sécurité des communications sur internet [8].

1.3.2.2 SSH (Secure Shell)

Est un protocole réseau qui permet aux administrateurs d'accéder à distance à un ordinateur, en toute sécurité. Tout comme SSL et TLS, SSH assure l'authentification des machines, la confidentialité et l'intégrité des données. Il assure aussi l'authentification des utilisateurs par mot de passe. Cependant, SSH est plus sécurisé que SSL et TLS en matière d'identification du client [8].

1.3.2.3 Certification X. 509

Un certificat électronique a pour objet de certifier une clé publique, La norme 509 permet de spécifier les formats des certificats à clé publique délivrés par les Autorités de Certification [1]. Le rôle de certificat est d'avoir une liste des certificats valides. Elle doit aussi révoquer les certificats expirés, douteux, etc. L'utilisateur se réfère cette autorité chaque fois qu'il veut contrôler la validité d'un certificat. Ces autorités sont organisées hiérarchiquement, de façon que la plus haute soit une autorité de

confiance maximale. Le rôle d'une autorité supérieure est de valider les autorités qui dépendent d'elle [2].

1.4 Systèmes de messagerie existants :

Utilisée aussi bien par les professionnels que les particuliers, la messagerie électronique est un outil de communication accessible depuis un ordinateur, un Smartphone ou une tablette, dès lors que l'utilisateur a accès à Internet. Dans un monde de plus en plus digitalisé, il est aujourd'hui presque inconcevable pour un étudiant ou un professionnel de ne pas posséder d'adresse électronique, d'autant plus que la création d'un compte de messagerie électronique est généralement gratuite, facile, et rapide [3]. Il existe plusieurs types de messagerie électronique dont chacun présente ses propres avantages par rapport aux autres selon le domaine d'utilisation, parmi ces principales messagerie on trouve : Outlook, Gmail, Yahoo [3].

- **Outlook.fr par Microsoft :** Il a été fondé par Jack Smith en1996 sous le nom de « Hotmail ». Il a ensuite été racheté par Microsoft et est devenu « MSN Hotmail » puis « Windows Live Hotmail ». L'objectif de son fondateur est de permettre aux utilisateurs d'accéder à leur messagerie électronique depuis n'importe quel ordinateur. Sabeer Bhatia voulait un nom avec « Mail » vers la fin, et il a choisi l'appellation « Hotmail ». Il est devenu l'un des premiers services de messagerie électronique, Hotmail se fonctionne avec une technologie Ajax [3].

- **Gmail de Google :** Avec Gmail, créer un compte est gratuit. Les messages sont consultables depuis un navigateur web ou une application mobile. L'adresse Gmail créée vous permet d'accéder à l'intégralité des services proposés par Google, comme YouTube, Google Store. Gmail en 2004, n'était accessible que par invitation. Il n'est devenu public que deux ans plus tard, avec un stockage de 1 Go seulement. Cette capacité de stockage a augmenté au fil des années. Gmail fait partie des services de messagerie électronique les

plus utilisés par les internautes, avec plus de 1,5 million d'utilisateurs actifs. Gmail associe les technologies Ajax et JavaScript. Il se base sur un système de filtres et de libellés afin d'automatiser les tâches dès qu'un courrier arrive [3].

- **Yahoo Mail de Yahoo :** Fondée en 1997, Yahoo Mail était l' ?uvre l'une entreprise américaine. Il s'agissait d'une application web qui permet d'envoyer des messages électroniques. Yahoo Mail permet d'effectuer des échanges de courriels, mais également de se constituer un carnet d'adresses et de profiter d'un calendrier. Vous pouvez également utiliser un bloc-notes. Yahoo Mail est plus qu'un service de messagerie électronique. Il s'agit avant tout d'un organisateur en ligne [3].

1.4.1 Avantages de la messagerie électronique

Outlook [4] :

- permet d'envoyer un mail à partir de Word : La fonction e-mailing est très intuitive grâce à la combinaison de Outlook et Word. Il suffit de taper le message sur Word et en quelques clics il sera transmis individuellement à toute ou partie de votre base de données.
- permet d'améliorer l'accessibilité : Les services Microsoft Office 365 ont la particularité d'être accessibles partout, tout le temps et sur n'importe quel appareil.
- donne accès à des services additionnels : En plus d'un service de messagerie professionnelle, Outlook Exchange c'est aussi une base de données Contact, un calendrier ainsi qu'une gestion des tâches et notes.
- consulter plusieurs boites de messagerie simultanément.

Gmail [5] :

- Un filtre anti-spam qui ne laisse passer aucun SPAM ;
- Outil de recherche performant ; la messagerie Gmail (liée à Google) dispose à

ce titre d'un outil de recherche en or pour retrouver n'importe quel mail en un temps record ;
- Services complémentaires : agenda en ligne, Google docs, carnet d'adresses ?

Yahoo [6] :
- Prenez un peu de code gratuit Obtenir applications Web fonctionne correctement dans tous les navigateurs peut être difficile. Yahoo, contrairement à certaines entreprises du Web, résout ce problème en donnant aux développeurs Web un accès gratuit à son immense utilisateur Yahoo Interface Library (YUI) ;
- Explorez méthodes de communication avancée : Bien que nous puissions envoyer des messages instantanés à partir de notre page Yahoo Mail, nous avons la possibilité d'installer Yahoo Messenger sur notre ordinateur et téléphone mobile. Avec elle, nous pouvons discuter avec d'autres via la voix et webcam ;
- Rechercher sur le Web en utilisant Yahoo : Comme Google, Yahoo indexe le Web et rend l'information à partir de pages Web disponibles pour les recherches Web.

1.5 Securité informatique

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Les objectifs de sécurité sont les suivants [22] :

- la disponibilité ;
- l'intégrité ;
- la confidentialité ;
- non-répudiation ;
- l'authentification.

La réalisation de fonctions de sécurité, telles que celles de gestion des identités, du contrôle d'accès, de détection d'intrusion par exemple, contribuent, via des mécanismes de sécurité comme le chiffrement par exemple, à satisfaire les exigences de sécurité exprimées en termes de disponibilité, d'intégrité, de confidentialité. Elles

concourent à la protection des contenus et des infrastructures numériques et sont supportées par des solutions techniques. Celles-ci sont à intégrer dans le système à sécuriser, en fonction du cycle de vie de ce dernier, par des approches complémentaires d'ingénierie et de gestion de la sécurité informatique.

- Disponibilité : La disponibilité d'une ressource est relative à la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la capacité d'une ressource à être utilisée (serveur ou réseau par exemple).
- Intégrité : Le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions, services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour contribuer à préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menace de corruption ou de destruction.
- Confidentialité : « La confidentialité est le maintien du secret des informations » (Le Petit Robert). Transposée dans le contexte de l'informatique et des réseaux, la notion de confidentialité peut être vue comme la « protection des données contre une divulgation nonnautorisée ».
- L'authentification :L'authentification doit permettre de vérifier l'identité d'une entité afin de s'assurer entre autres, de l'authenticité de celle-ci. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une information spécifique qu'elle est censée être seule à détenir telle que, par exemple, un mot de passe ou une empreinte biométrique. Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'dentification, l'authentification des entités et la gestion des droits et permissions associées aux personnes . Cela exclut l'usage anonyme des ressources. C'est également sur la base de l'identification des personnes et des accès aux ressources que s'établissent des fonctions de facturation et de surveillance.
- Non-répudiation : La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu. À ce critère de sécurité

peuvent être associées les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité. L'imputabilité se définit par l'attribution d'une action (un événement) à une entité déterminée (ressource, personne). Elle peut être réalisée par un ensemble de mesures garantissant l'enregistrement fiable d'informations pertinentes par rapport à une entité et à un événement. L'établissement de la responsabilité d'une personne vis-à-vis d'un acte dans le monde de l'informatique et des télécoms nécessite l'existence de mesures d'authentification des individus et d'imputabilité de leurs actions. La traçabilité permet de suivre la trace numérique laissée par la réalisation d'un événement (message électronique, transaction commerciale, transfert de données). Cette fonction comprend l'enregistrement des événements, de la date de leur réalisation et leur imputation. Elle permet, par exemple, de retrouver l'adresse IP d'un système à partir duquel des données ont été envoyées.

1.6 Conclusion

A l'issu de ce chapitre, nous avons donné une brève définition sur la messagerie, son architecture et son fonctionnement, aussi les composants de système de messagerie, et juste après nous avons défini les différents protocoles de sécurité liée aux systèmes de messagerie électronique qui sont en relation avec notre travail. Nous pouvons entamer la phase de présentation de notre travail dans le prochain chapitre, qui consiste à la modélisation du système et cela à l'aide de différents diagrammes de modélisation du langage UML.

Chapitre 2

Analyse et conception

2.1 Introduction

La phase de conception est la première étape dans la réalisation d'un projet, elle doit d'écrire de manière non ambiguë le fonctionnement futur du système, afin d'en faciliter la réalisation. Dans ce chapitre, nous allons suivre une méthode d'analyse et de conception qui permet de formaliser les étapes préliminaires du développement d'un système afin de le rendre plus fidèle aux besoins des utilisateurs.

2.2 Modélisation UML

2.2.1 Langage UML

UML (Unified Modeling Language), se définit comme un langage de modélisation graphique et textuel destiné à comprendre et à définir des besoins, spécifier et documenter des systèmes, esquisser des architectures logicielles, concevoir des solutions et communiqduer des points de vue. UML modélise l'ensemble des données et des traitements en élaborant des différents diagrammes [28].

2.2.2 Diagrammes UML

UML dans sa version 2 comporte treize types de diagrammes, qui permettent de définir une application selon plusieurs points de vue. Ces diagrammes sont regroupés dans deux grands ensembles : les diagrammes structurels (statiques) et les diagrammes de comportement [25]

- **Diagrammes structurels :** ces diagrammes, au nombre de six, ont vocation à représenter l'aspect statique d'un système (classes, objets, composant).
- **Diagrammes de comportement :** ces diagrammes représentent la partie dynamique d'un système réagissant aux événements et permettant de produire les résultats attendus par les utilisateurs. Sept diagrammes sont proposés par UML 2.

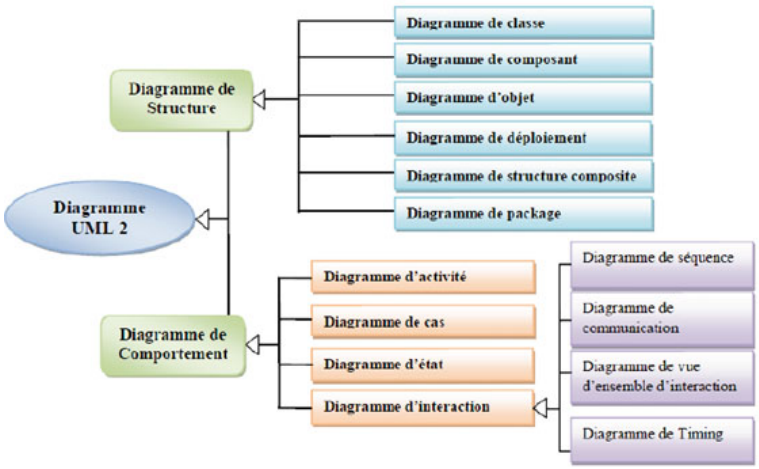


FIGURE 2.1 – Les diagrammes UML [23].

2.2.2.1 Diagramme de classe

Les diagrammes de classes sont généralement considérés comme les plus importants dans un développement orienté objet. Ils représentent l'architecture conceptuelle du système : ils décrivent les classes que le système utilise, les relations entre objets, les attributs, et les opérations qui caractérisent chaque classe d'objets [20].

2.2.2.2 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation représente la structure des grandes fonctionnalités nécessaires aux utilisateurs du système. C'est le premier diagramme du modèle UML, celui où s'assure la relation entre l'utilisateur (humain ou machine) et les objets que le système met en oeuvre [26].

2.2.2.3 Diagrammes de séquence

Un diagramme de séquences est un diagramme d'interaction qui expose en détail la façon dont les opérations sont effectuées : quels messages sont envoyés et quand ils le sont. Les diagrammes de séquences sont organisés en fonction du temps qui s'écoule au fur et à mesure que nous parcourons la page. Les objets impliqués dans l'opération sont répertoriés de gauche à droite en fonction du moment où ils prennent part dans la séquence [16].

2.3 Processus unifié :

2.3.1 Processus unifié

Un processus définit une séquence d'étapes, en partie ordonnées, qui concourent à l'obtention d'un système logiciel ou à l'évolution d'un système existant [27]. Un processus unifié est un processus de développement logiciel construit sur UML ; il est itératif et incrémental, centré sur l'architecture, conduit par les cas d'utilisation et piloté par les risques. [27] L'objectif du Processus unifié est de guider les développeurs vers l'implémentation et le déploiement efficaces de systèmes répondant aux besoins des clients [24].

2.4 Spćification des besoins

L'application envisagée doit satisfaire les besoins fonctionnels qui seront exécutés par le système et les besoins non fonctionnels qui perfectionnent la qualité logicielle du système.

2.4.1 Besoins fonctionnels

Les besoins fonctionnels ou besoins métiers représentent les actions que le système doit exécuter, il ne devient opérationnel que s'il les satisfait. Cette application doit couvrir principalement les besoins fonctionnels suivants :

2.4.1.1 Besoins de point de vue utilisateur

- Gestion de profil ;
- Authentification des utilisateurs ;
- Rédiger des messages, leurs attacher des fichiers joints, et les expédier ;
- Chiffrer les message à envoyés ;
- Consulter les messages qui lui sont destiné et les messages envoyés ;
- Se déconnecter (quitter l'application).

2.4.1.2 Besoins de point de vue administrateur

- Gérer des comptes utilisateurs.

2.4.2 Besoins non fonctionnels

Ce sont des exigences qui ne concernent pas spécifiquement le comportement du système mais plutôt identifient des contraintes internes et externes du système. Les principaux besoins non fonctionnels de notre application se résument comme suit :

- **Fiabilité :**Garantir l'intégrité et la cohérence des données à chaque mise à jour et à chaque insertion ;

- **Les erreurs :** Les ambigüités doivent être signalées par des messages d'erreurs bien organisés pour bien guider l'utilisateur ;
- **L'ergonomie :** l'application offre une interface conviviale et facile à utiliser. La manipulation de l'interface ne doit pas nécessiter des connaissances poussées en informatique, elle doit être simple et claire afin de s'adapter aux connaissances informatiques des utilisateurs ;
- **La sécurité :** chiffrerement des message permet d'assurée la confidentialité et l'intégrité des donnée anisi l'authentification ;
- **Robustesse et maintenabilité** : l'application doit permettre le stockage des informations concernant tous les internautes inscrits et les différents traitements utiles pour le fonctionnement correct, ainsi qu'assurer une gestion exhaustive des erreurs ;
- Le code doit être clair pour permettre des futures évolutions ou améliorations.

2.4.3 Diagramme de cas d'utilisation

A chaque cas d'utilisation doit être associ ée une description textuelle des interactions entre l'acteur et le système et les actions que le système doit r éaliser en vue de produire les r ésultats attendus par les acteurs [21]. Pour exprimer les cas d'utilisations de notre système, nous avons choisi le formalisme suivant :

Numéro du cas d'utilisation	**Nom de cas d'utilisation**
Résumé	But de cas d'utilisation
Acteurs	Acteurs participants au cas d'utilisation
Pré-condition	L'utilisateur doit avoir un compte
Scénario nominal	Séquence d'actions normales associées au cas d'utilisation
Alternative Exception	Séquence d'actions alternatives pouvant conduire également à un succès. Séquence d'actions conduisant à un échec.

TABLE 2.1 – Formalisme de description des cas d'utilisation

2.4.4 Diagramme globale des cas d'utilisations

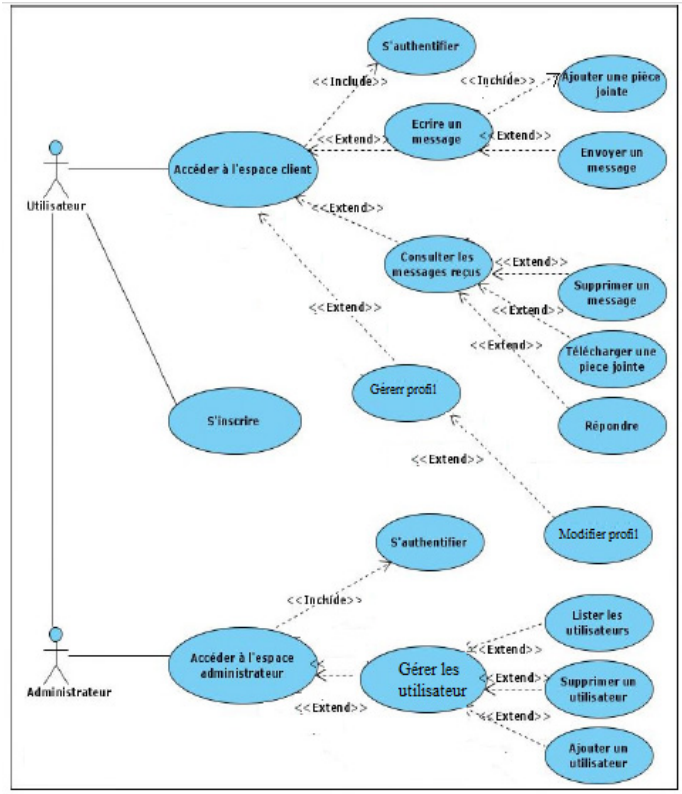


FIGURE 2.2 – Diagramme globale des cas d'utilisations associé aux acteurs

2.4.5 Cas d'utilisations Gérer les utilisateurs

Cas d'utilisation N 1	**Gérer les utilisateurs**
Résumé	Gérer les utilisateurs
Acteurs	Administrateur
Pré-condition	L'administrateur s'authentifier.
Scénario nominal	[début] 1. Accès à l'application 2. S'authentifier ; 3. L'administrateur demande le formulaire de gestion des utilisateurs ; 4. Le système affiche le formulaire ; 5. l'administrateur effectue l'action souhaitée (ajout, suppression) ; Pour l'ajout : – Si les champs sont incomplets Alors Exécuter l'exception ; – Sinon Aller à (6) ; 6. Confirmer l'action ; [fin]
Alternative Exception	Le système affiche un message d'erreur et réaffiche le formulaire d'ajout et attend que l'administrateur ressaisisse ses informations.

TABLE 2.2 – Description du cas d'utilisation ≪ Gérer les utilisateurs ≫

2.4.6 Cas d'utilisation Envoyer un message

Cas d'utilisation N 2	**Envoyer un message**
Résumé	permet aux utilisateurs d'écrire un nouveau message pour pouvoir l'envoyer, lui attacher une pièce jointe .
Acteurs	Utilisateur
Pré-condition	Authentification
Scénario nominal	[début] 1. L'utilisateur accède à ≪nouveau message ≫,il choisit le destinataire, écrit l'objet du message anfin il ajoute une pièce jointe(le message chiffré). 2. Le système vérifie le contenu de message à envoyer. – Si les champs sont incomplets Alors Exécuter l'exception ; – Si non il envoie le message au serveur via le socket client pour l'enregistrer dans la base de données. Le récepteur pourra récupérer le message au moment de sa connexion. [fin]
Alternative Exception	Le système affiche un message d'erreur.

TABLE 2.3 – Description du cas d'utilisation ≪ Envoyer des messages ≫

FIGURE 2.3 – Diagramme du cas d'utilisation ≪ Envoyer un message ≫

2.4.7 Cas d'utilisation s'authentifier

Cas d'utilisation N 1	**S'authentifier**
Résumé	Vérification de l'identité des utilisateurs (Login et mot de passe).
Acteurs	Utilisateur
Pré-condition	L'utilisateur doit avoir un compte

Scénario nominal	[début] 1. Demande de connexion ; 2. Le système affiche le formulaire d'authentification ; 3. L'utilisateur saisit son login et son mot de passe ; – Si les champs sont incomplets Alors Exécuter l'exception ; – Sinon Aller à (4) ; 4. Le système vérifie la validité des informations fournies ; – Si les champs sont incorrects Alors Exécuter l'exception ; – Sinon Aller à (5) ; 5. Le système donne l'accès à l'interface correspondante. [fin]
Alternative Exception	Le système affiche un message d'erreur pour ressaisir les informations.

TABLE 2.4 – Description du cas d'utilisation ≪ S'authentifier ≫

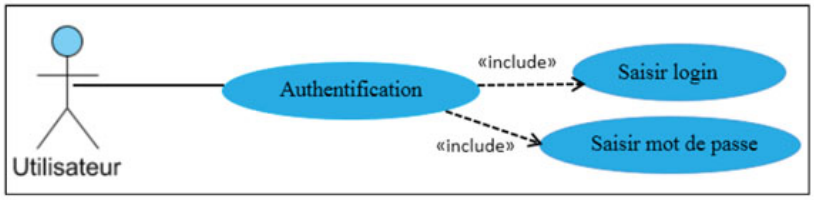


FIGURE 2.4 – Diagramme du cas d'utilisation ≪ authentification ≫

2.4.8 Cas d'utilisation Inscription

Cas d'utilisation N 4	**Inscription**
Résumé	Permet à l'utilisateur de s'inscrire
Acteurs	Utilisateur
Pré-condition	Aucune
Scénario nominal	[début] 1. Demande de formulaire d'inscription ; 2. L'utilisateur saisit ses informations puis valide ; 3. Le système vérifie la conformité des informations fournies ; – Si les informations fournies sont incomplètes ou incorrectes Alors Exécuter l'exception ; [fin]
Alternative Exception	Le système réaffiche le formulaire d'authentification d'inscription et attend que l'utilisateur ressaisisse les informations.

TABLE 2.5 – description du cas d'utilisation ≪ Inscription ≫

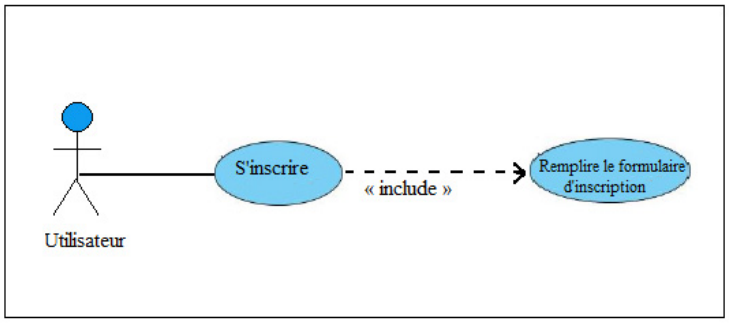


FIGURE 2.5 – Diagramme de cas d'utilisation ≪ Inscription ≫

2.5 Conception

La conception c'est la phase qui permet de décrire la maniéré dont le systèm doit être construit. Pour cela, nous allons établire les diagrammes de séquences et le diagramme de classe qui permettront de décrire les fonctionnalités obtenu durant la phase d'analyse. Les diagrammes suivants sont la représentation graphique des interactions entre les acteurs et le système selon un ordre chronologique.

2.5.1 Diagrammes de séquences

2.5.1.1 Diagramme de séquence du cas d'utilisation Inscription

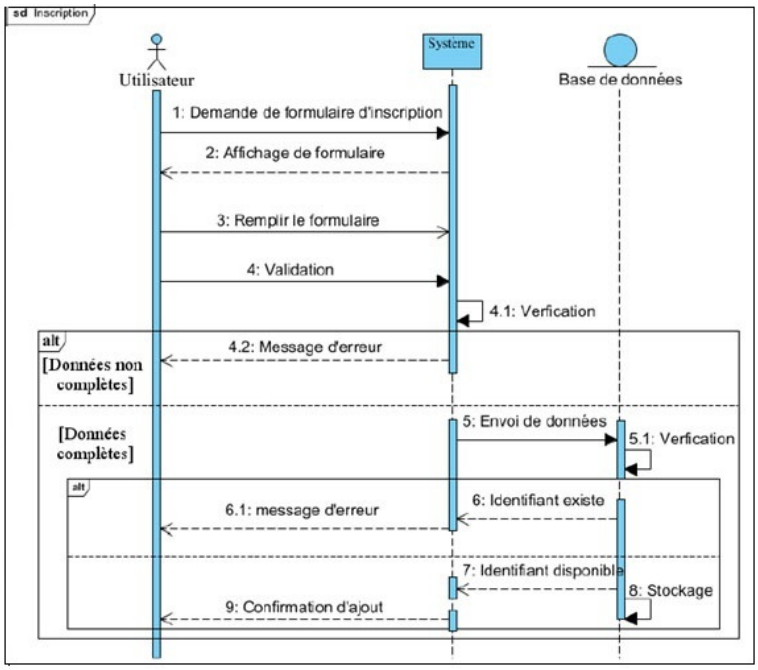


FIGURE 2.6 – Diagramme de séquence du cas d'utilisation ≪ S'inscrire ≫

2.5.1.2 Diagramme de séquence du cas d'utilisation authentification

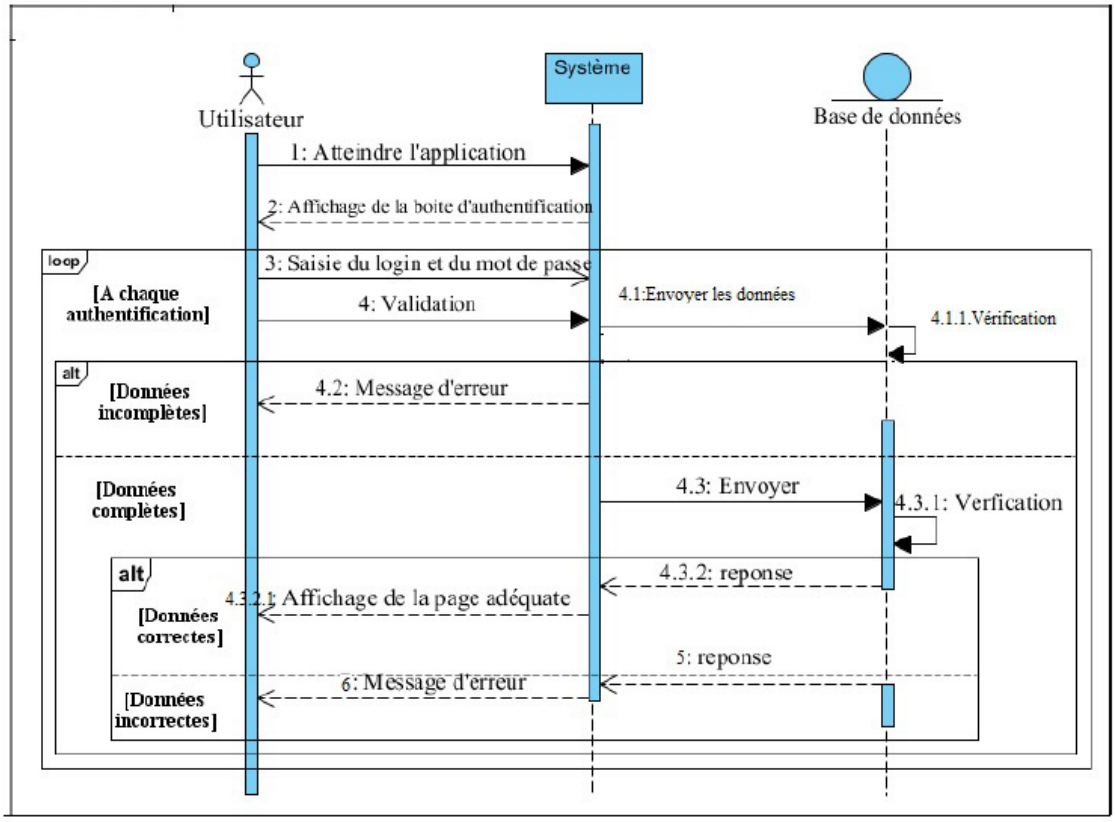


FIGURE 2.7 – Diagramme de séquence du cas d'utilisation ≪ s'authentifier ≫

2.5.1.3 Diagramme de séquence du cas d'utilisation Envoyer un message

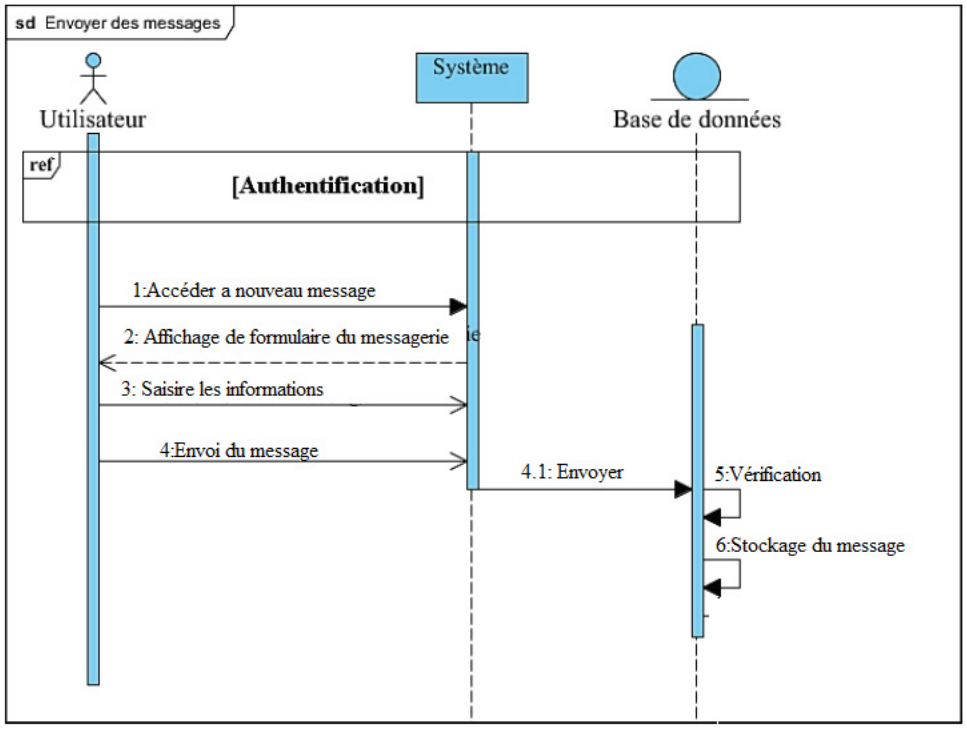


FIGURE 2.8 – Diagramme de séquence du cas d'utilisation ≪ Envoyer un message ≫

2.5.1.4 Diagramme de séquence du cas d'utilisation Lire/ supprimer les messages reçus

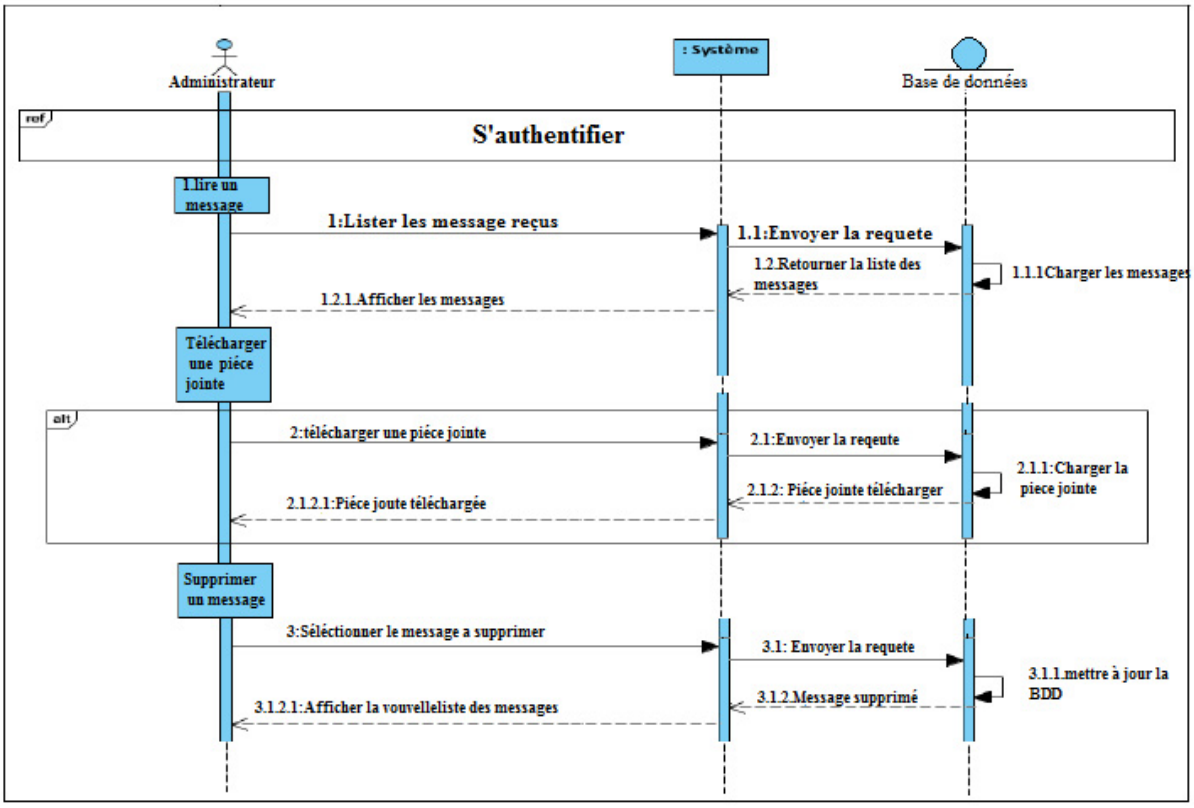


FIGURE 2.9 – Diagramme de séquence du cas d'utilisation ≪ Lire/ supprimer les messages reçus ≫

2.5.1.5 Digramme de séquence du cas d'utilisation Gérer les utilisateurs

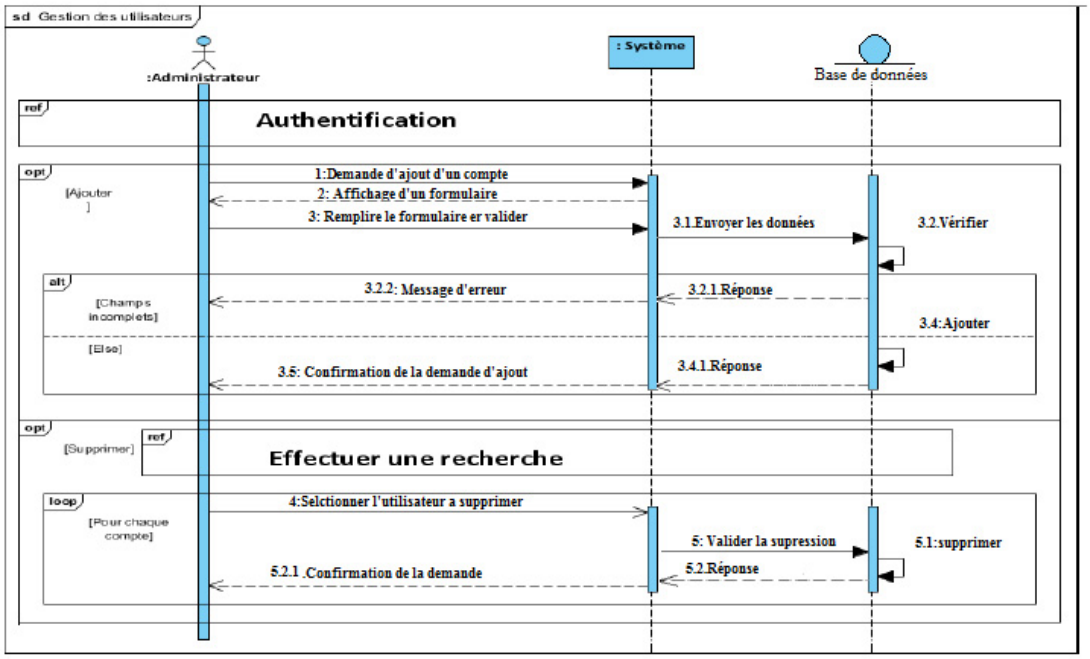


FIGURE 2.10 – Diagramme de séquence du cas d'utilisation ≪ Gérer les utilisateurs ≫

2.5.2 Diagramme de classe générale

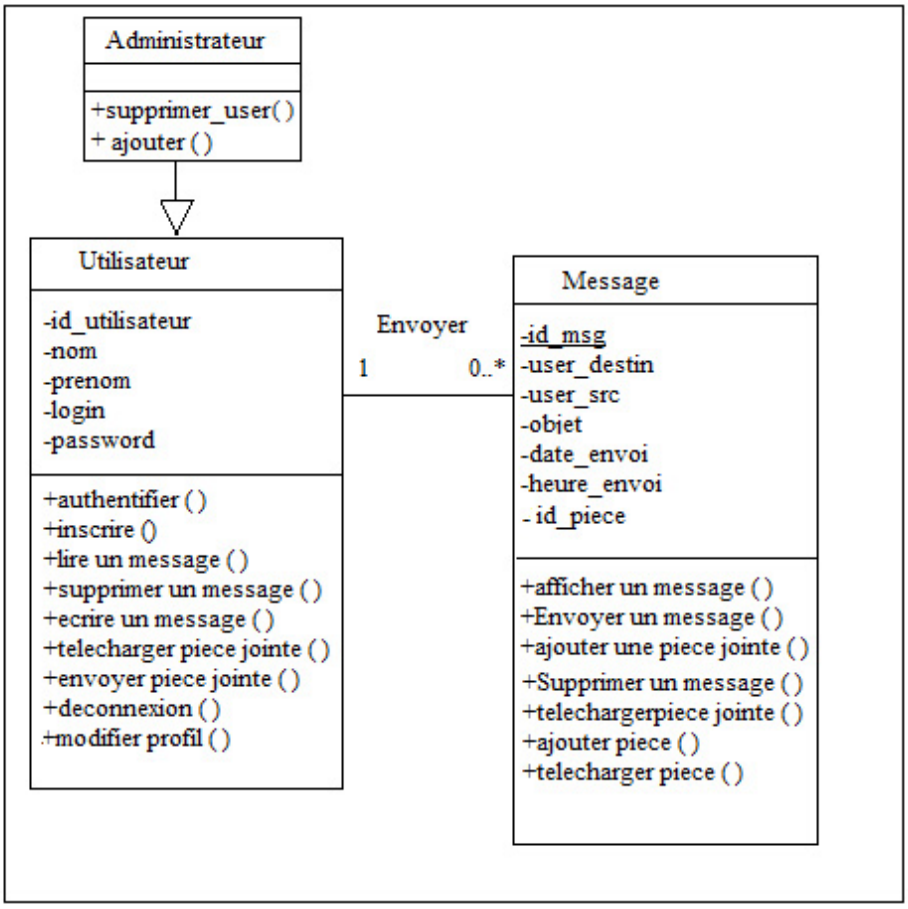


FIGURE 2.11 – Diagramme de classe

2.6 Régle de passage d'un modéle de classes à un modéle relationnel

- **Règle 1 [29] :** Transformation des classes : Chaque classe du diagramme UML devient une relation. Il faut choisir un attribut de la classe pouvant jouer le rôle de l'identifiant. Dans le cas où aucun attribut ne convient en tant

qu'identifiant, il faut en ajouter un de telle sorte que la relation dispose d'une clé primaire.

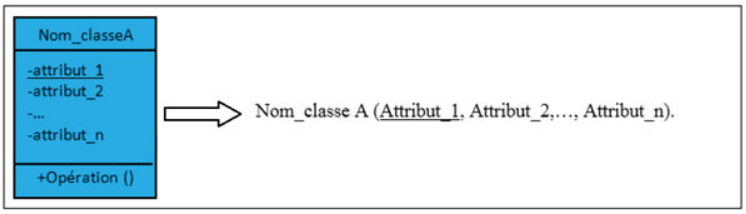


FIGURE 2.12 – Règle 1 : Transformation des classes [29]

- **Règle 2 [29] :** Association un- à -plusieurs : Il faut ajouter un attribut de type clé étrangère dans la relation fils de l'association. L'attribut porte le nom de la clé primaire de la relation pére de l'association.

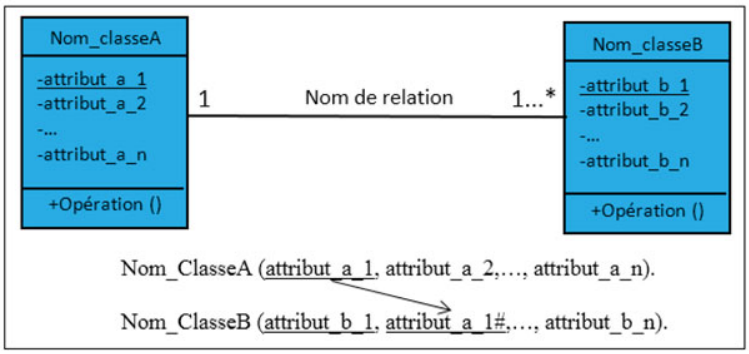


FIGURE 2.13 – Règle 2 : Association un- à -plusieurs [29]

- **Règle 3 [29] :** Association un-à-un Il faut ajouter un attribut clé étrangère dans la relation dé rivée de la classe ayant la multiplicité minimale égale à un. L'attribut porte le nom de la clé primaire de la relation dérivée de la classe connectée à l'association. Si les deux cardinalités (multiplicités) minimales sont à zéro, le choix est donné entre les deux relations dérivées de la régle R1. Si les deux cardinalités minimales sont à un, il est sans doute préférable de fusionner les deux entités (classes) en une seule.

- **Règle 4 [29] :** Transformation d'héritage
  Trois décompositions sont possibles pour traduire une association d'héritage en fonction des contraintes existantes :

  1. **Décomposition par distinction :** il faut transformer chaque sous-classe en une relation. La clé primaire de la sur-classe, migre dans la (les) relation(s) issue(s) de la (des) sous-classe(s) et devient à la fois clé primaire et clé étrangère.
  2. **Décomposition descendante (push-down)** : s'il existe une contrainte de totalité ou de partition sur l'association d'héritage, il est possible de ne pas traduire la relation issue de la sur-classe. Il faut alors faire migrer tous ses attributs dans la (les) relation(s) issue(s) de la (des) sous-classe(s).
  3. **Décomposition ascendante (push-up) :** il faut supprimer la (les) relation(s) issue(s) de la (des) sous-classe(s) et faire migrer les attributs dans la relation issue de la sur classe.

2.6.1 Modèle relationnel

- Administrateur (#id_utilisateur)
- Utilisateur (id_utilisateur, nom, prenom, login, password)
- Message (id_msg, user_destin, user_src, objet, date_envoi, heure_envoi, id_piece, #id_utilisateur)

2.7 Conclusion

Ce chapitre nous a permis de présenter le langage de modalisation UML et le processus de développement unifié (Unified Processus). Ensuite on a déterminé le cadre du projet de réalisation de l'application et de définir les besoins, en identifiant toutes les entités internes qui vont interagir avec le système (acteurs). Nous avons présent les différents diagrammes de séquence d'interaction constitues notre application. Ensuite, nous avons recensé les concepts de base du diagramme de classes ainsi que les règles de modélisation, les règles de passage d'un diagramme de classes

vers le modèle relationnelle qui nous permet d'avoir le schéma de la base de données de l'application à réaliser. Cela fait la base pour la phase réalisation tel qu'en vas garantir la fiabilité et l'efficacité de l'application à réaliser.

Chapitre 3

REALISATION

3.1 Introduction

L'étape de réalisation est la dernière de notre projet, elle se présente comme étant l'étape la plus cruciale vu qu'elle traite l'onglet pratique du projet. Ce chapitre est consacré à la réalisation et la mise en oeuvre de notre application, nous allons présenter les outils de développement adoptés, soit l'environnement utilisé et aussi notre système de messagerie électronique et cela en illustrant les principaux interfaces et fenêtres de l'application.

3.2 L'environnement de développement

3.2.1 Langages de programmation

les deux languages de programmation utilisés sont les suivants :

3.2.1.1 Le langage SQL

SQL signifie " Structured Query Language " c'est-à-dire " Langage d'interrogation Structuré ".En fait SQL est un langage complet de gestion de bases de données relationnelles. L'accès aux BDD (bases de données) se fait de façon standard à l'aide de requêtes du langage SQL. Il existe un outil d'administration, PhpMyAdmin, qui

nous offre une interface pour manipuler les tables. La connaissance de quelques requêtes permet de répondre à la majorité des besoins de programmation[30].

3.2.1.2 Le langage PHP

PHP est un langage de programmation informatique essentiellement utilisé pour produire à la volée des pages web dynamiques. Dans sa version 5 lancée en juillet 2004, PHP s'est imposé comme le langage de référence sur le web en raison de sa simplicité, de sa gratuité et de son origine de logiciel libre. PHP est considéré par certains comme une plateforme de développement en raison de l'étendue et de la richesse de sa bibliothèque. [31]

3.2.2 Outils de programmation

les outils de programmation utilisés dans la réalisation sont :

3.2.2.1 Netbeans IDE 8.0.2

NetBeans est un environnement de développement intégré, permet de supporter différents autres langages, comme C, C++, JavaScript, XML, PHP et HTML. Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, éditeur graphique d'interfaces et de pages Web, analyseurs de code, et les convertisseurs). NetBeans constitue par ailleurs une plateforme utilisée comme brique logicielle pour la création d'applications spécifiques (bibliothèque Swing (Java)). Les partenaires privilégiés fournissent des modules à valeurs rajoutées qui s'intègrent facilement à la Plateforme et peuvent être utilisés pour développer ses propres outils et solutions.[32]

3.2.2.2 MySQL

(My Structured Query Language) est un système de gestion de base de données Relationnelles (SGBDR) et basé sur un modèle client - serveur. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde. Son rôle consiste

à stocker et à gérer une grande quantité de données en les organisant sous forme de tables. Le système MySQL doit aussi permettre la manipulation de ces donnéesà travers le langage standard du traitement des bases de données SQL. Les bases de données MySQL sont accessibles en utilisant les langages de programmation, Java, Perl, etc [33]

3.2.2.3 PhpMyAdmin

PHPMyAdmin est un logiciel libre, écrit en PHP destiné à gérer l'administration de MySQL sur le World Wide Web . PhpMyAdmin supporte une large gamme d'opérations avec MySQL. Les opérations les plus fréquemment utilissé sont pris en charge par l'interface utilisateur (bases de données de gestion, tables, champs, relations, les index, les utilisateurs, les permissions), alors que vous avez toujours la possibilité d'exécuter directement une instruction SQL. PhpMyAdmin permet de faire toutes sortes d'opérations comme : Créer et détruire des bases de données (à condition d'avoir les droits) ; Créer, détruire et modifier la description des tables ; Consulter le contenu des tables, modifier certaines lignes ou le détruire [34].

3.2.2.4 Notpad++

est un éditeur de texte générique codé en C ++, qui intégre la coloration syntaxique de code source pour les langages et fichiers C, C ++, Java, XML, HTML, PHP, JavaScript[35]

3.2.3 Outils de d'éveloppements

s

3.2.3.1 gpg4win-3.1.11

Gpg4win est un logiciel de chiffrement de fichiers et d'e-mails fonctionnant sous la plupart des versions de Microsoft Windows. Il utilise le système de chiffrement asymétrique de GNU Privacy Guard (GPG) pour chiffrer et signer. [37]

3.2.3.2 kleopatra

Kleopatra est une interface pour le logiciel de chiffrement GnuPG. Pour la plupart des actions il faut une clé publique (certificat) ou une clé privée. La clé secrète est nécessaire pour déchiffrer ou signer. La clé publique peut être utilisée pour le chiffrement des messages at aussi pour vérifier l'identité. [38]

3.3 Principales interfaces

Dans ce qui suit, nous allons présenter les interfaces de notre application.

3.3.1 Interface d'authentification

La page d'authentification permet à un client qui est déjà inscrit de s'authentifier pour accéder à l'application. Une fois ses informations sont correctes, le système affiche la page appropriée (page d'accueil). Dans le cas contraire, le système réaffiche la page d'authentification avec un message d'erreur.

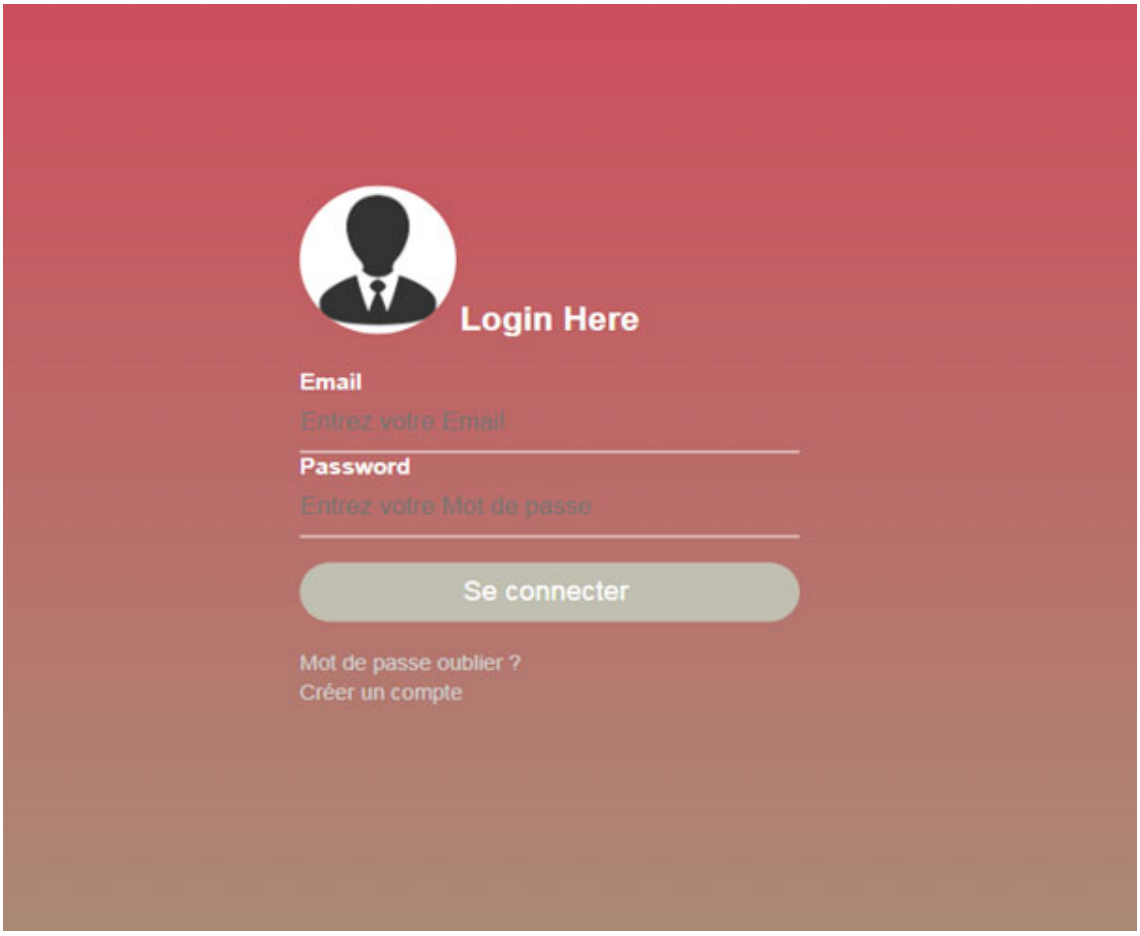


FIGURE 3.1 – Interface d'authentification d'un client

3.3.2 Interface d'inscription

L'interface suivante permet à un utilisateur de creér un nouveau compte, il suffit de remplire tous les champs de formulaire.

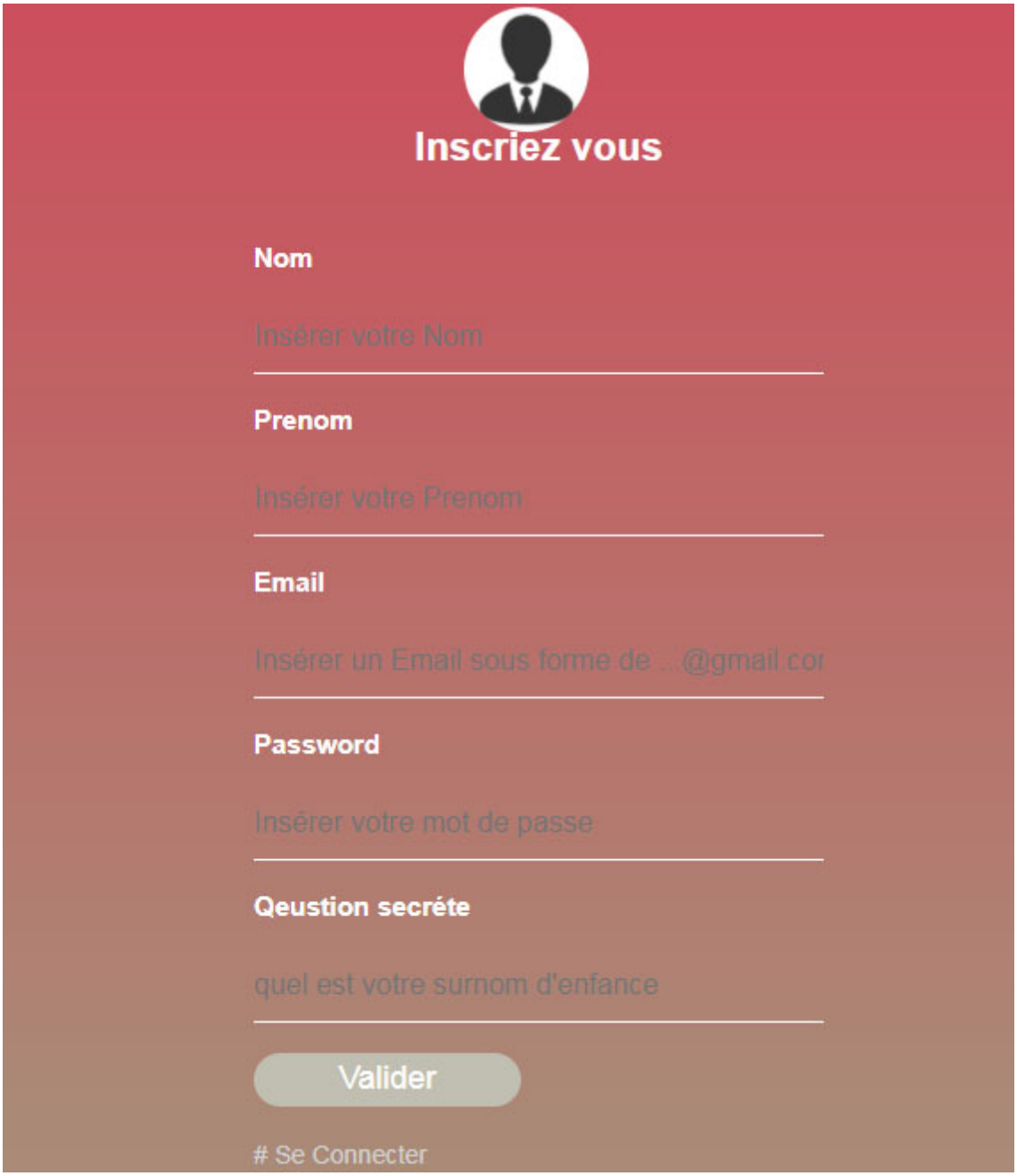


FIGURE 3.2 – Interface d'inscription

3.3.3 Interface d'accueil

Une fois le client est authentifié, le système affiche la page d'accueil, Dans cette page, le client peut consulter les messages reçus (Réception) ou les messages envoyés (Envoyé), envoyer un nouveau message(Nouveau), consulter son profil (cliquer sur son nom qui s'affiche en haut a droite) et en fin quitter la page(Déconnecter).

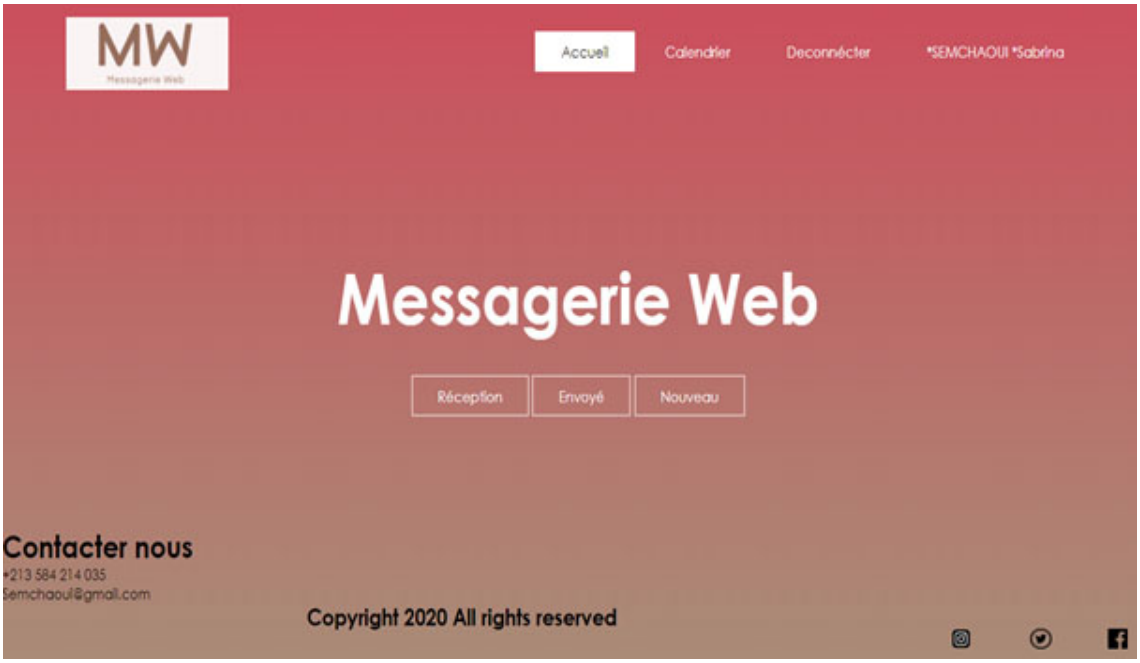


FIGURE 3.3 – Interface d'accueil

3.3.4 Boite de réception

Un message est envoyé sous forme d'une pièce jointe, le client peut lire les messages, si la pièce jointe n'a pas l'extension ≪.gpg ≫, sinon il doit la télécharger et la déchiffrer on utilisant sa clé privée, comme il peut supprimer le message.

FIGURE 3.4 – interface de la boite de réception

3.3.5 Interface messages envoyés

Cette page permet à l'utilisateur de consulter ou de supprimer les messages envoyés.

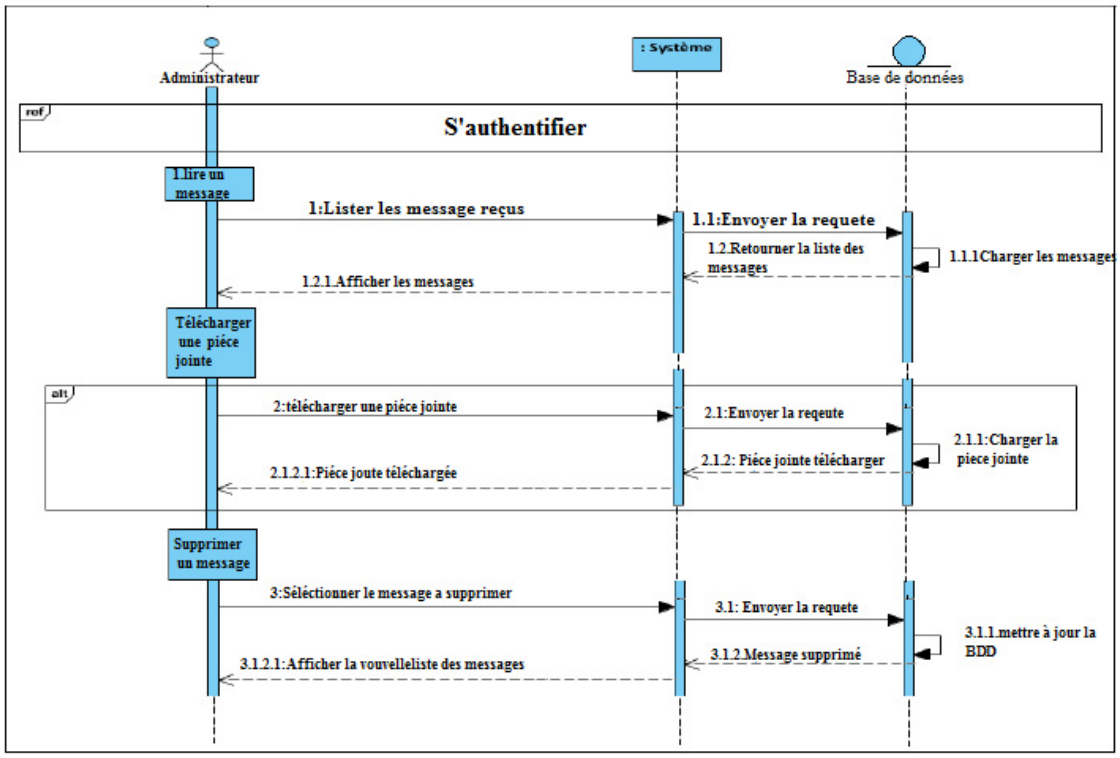


FIGURE 3.5 – Interface messages envoyés

3.3.6 Interface nouveau message :

Dans cette page, le client peut envoyer un message a un destinataire, il suffit de choisir le login correspond qui se trouve dans une liste, puis attacher une piece jointe à son message (choisir un fichier).

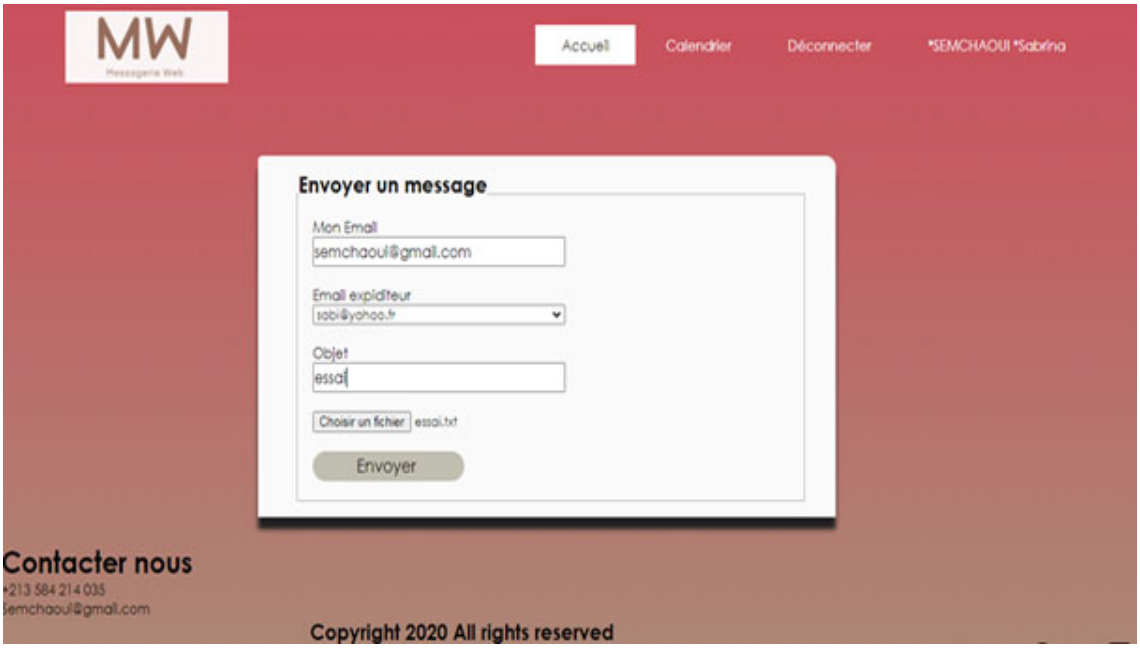


FIGURE 3.6 – Interface message nouveau

3.3.7 Interface d'administration ≪ gestion des utilisateurs ≫

Les interfaces suivante permettent à l'administrateur d'ajouter et de supprimer un compte d'utilisateur :

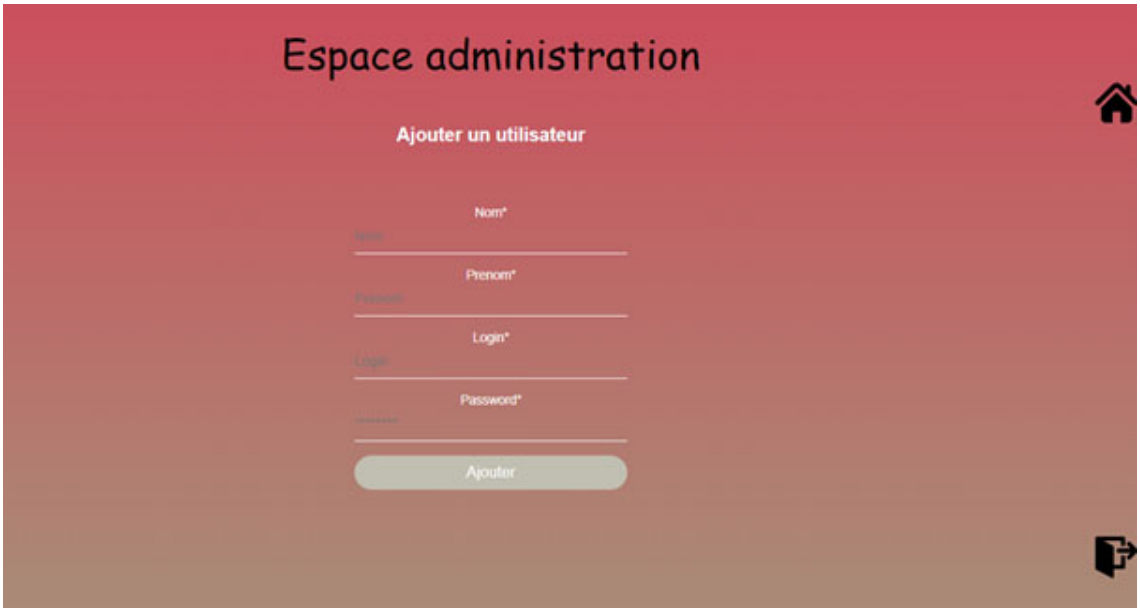


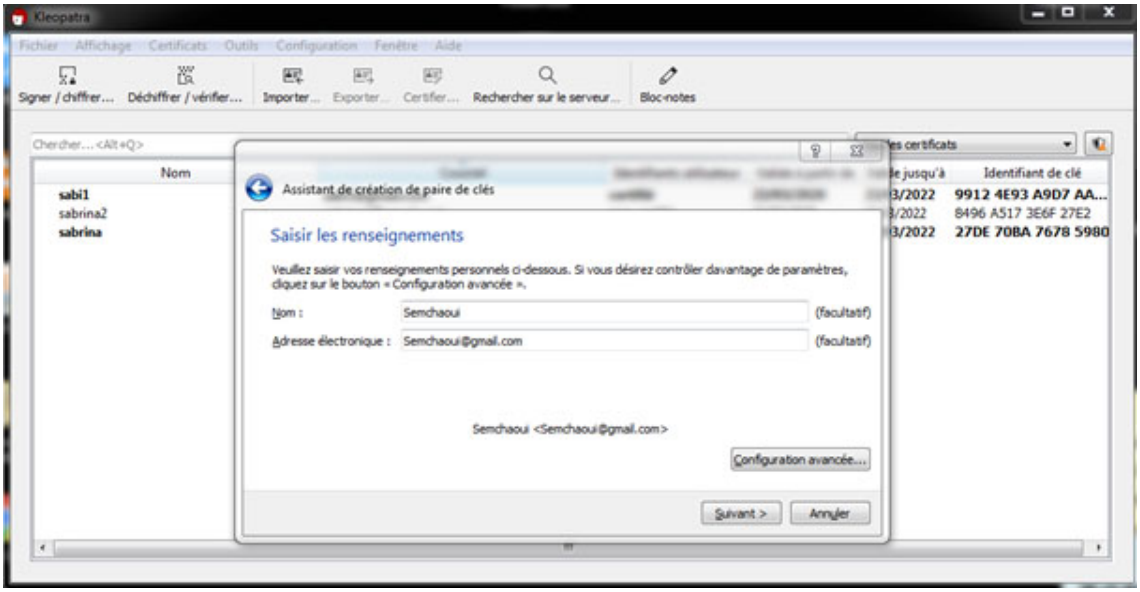
FIGURE 3.7 – Interface pour l'ajout d'utilisateurs

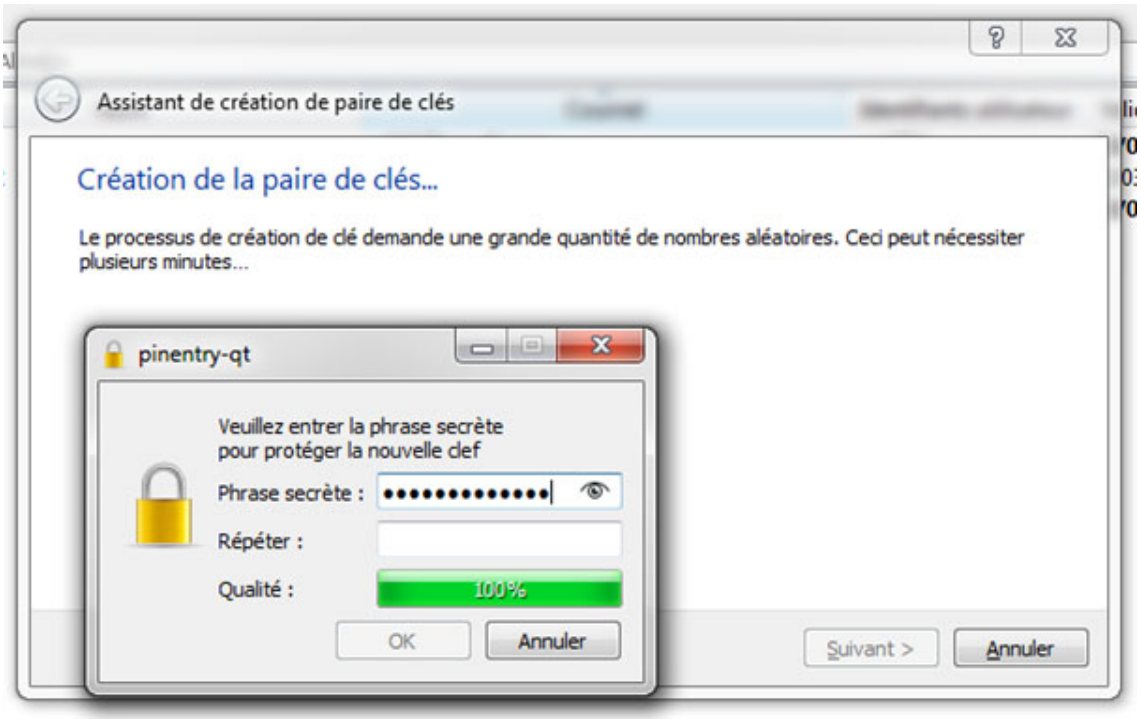
FIGURE 3.8 – Interface pour la suppression d'utilisateurs

3.3.8 Chiffrement

3.3.9 Créer une paire de clé

les interfaces suivantes reperesentent les étapes pour générer une paire de clé.




Assistant de création de paire de clés
Création de la paire de clés...
Le processus de création de clé demande une grande quantité de nombres aléatoires. Ceci peut nécessiter plusieurs minutes...
pinentry-qt
Veuillez entrer la phrase secrète pour protéger la nouvelle clef
Phrase secrète :
Répéter :
Qualité :
100%
OK
Annuler
Suivant >
Annuler

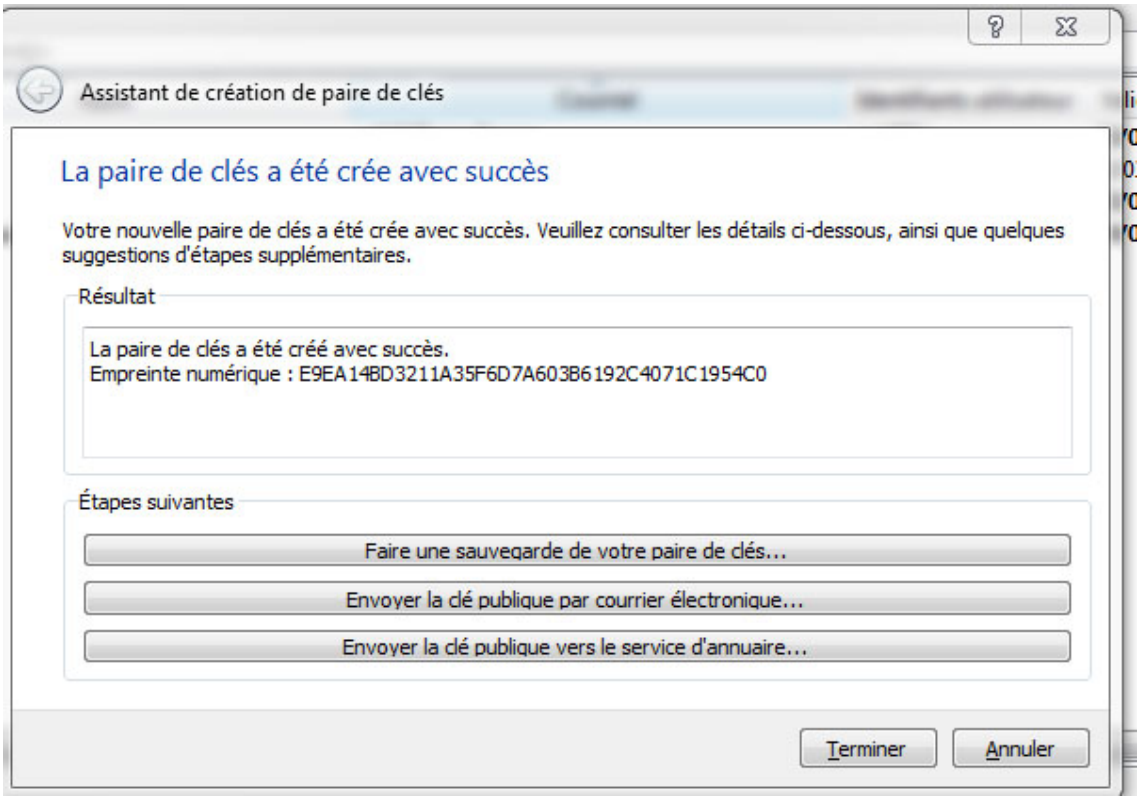
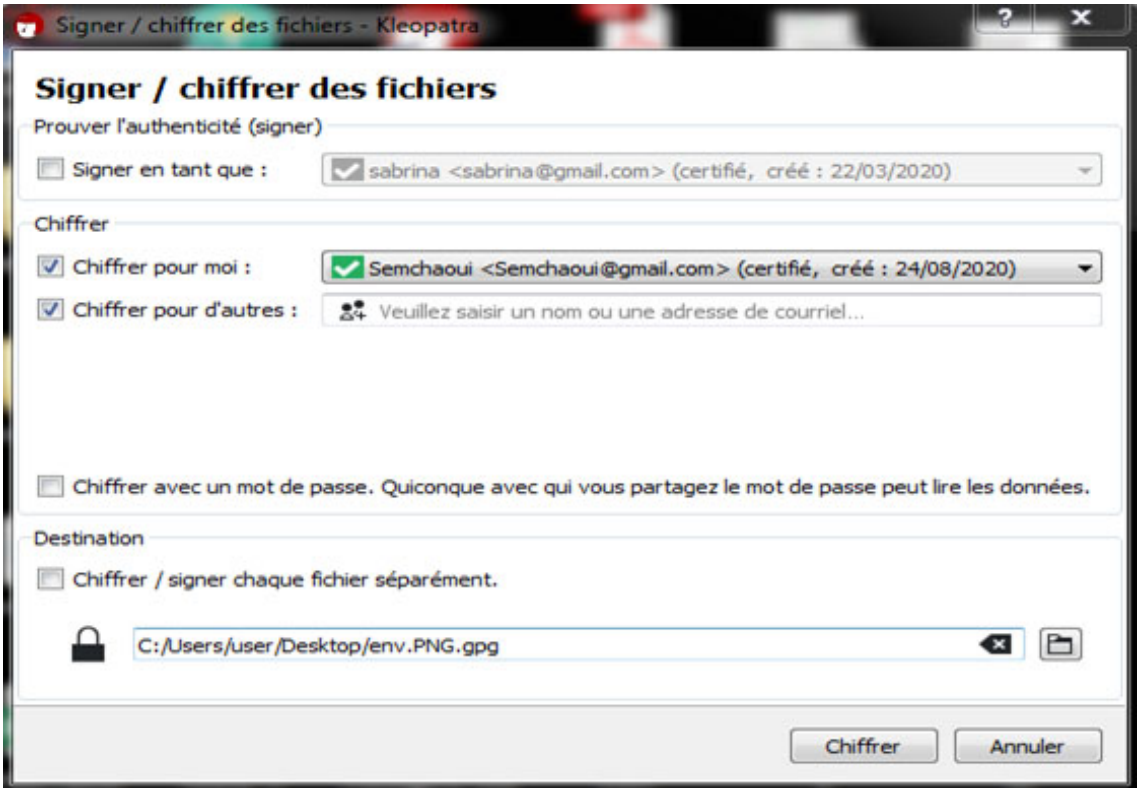


FIGURE 3.9 – Interface de géneration des clés

3.3.10 Chiffrer un fichier

L'utilisateur doit chiffrer le message à envoyé avac la clé public de destinatire ; comme elles représentent les figures suivantes.


Signer / chiffrer des fichiers - Kleopatra
Signer / chiffrer des fichiers
Prouver l'authenticité (signer)
Signer en tant que :
sabrina <sabrina@gmail.com> (certifié, créé : 22/03/2020)
Chiffrer
Chiffrer pour moi :
Semchaoui <Semchaoui@gmail.com> (certifié, créé : 24/08/2020)
Chiffrer pour d'autres :
Veuillez saisir un nom ou une adresse de courriel...
Chiffrer avec un mot de passe. Quiconque avec qui vous partagez le mot de passe peut lire les données.
Destination
Chiffrer / signer chaque fichier séparément.
C:/Users/user/Desktop/env.PNG.gpg
Chiffrer
Annuler

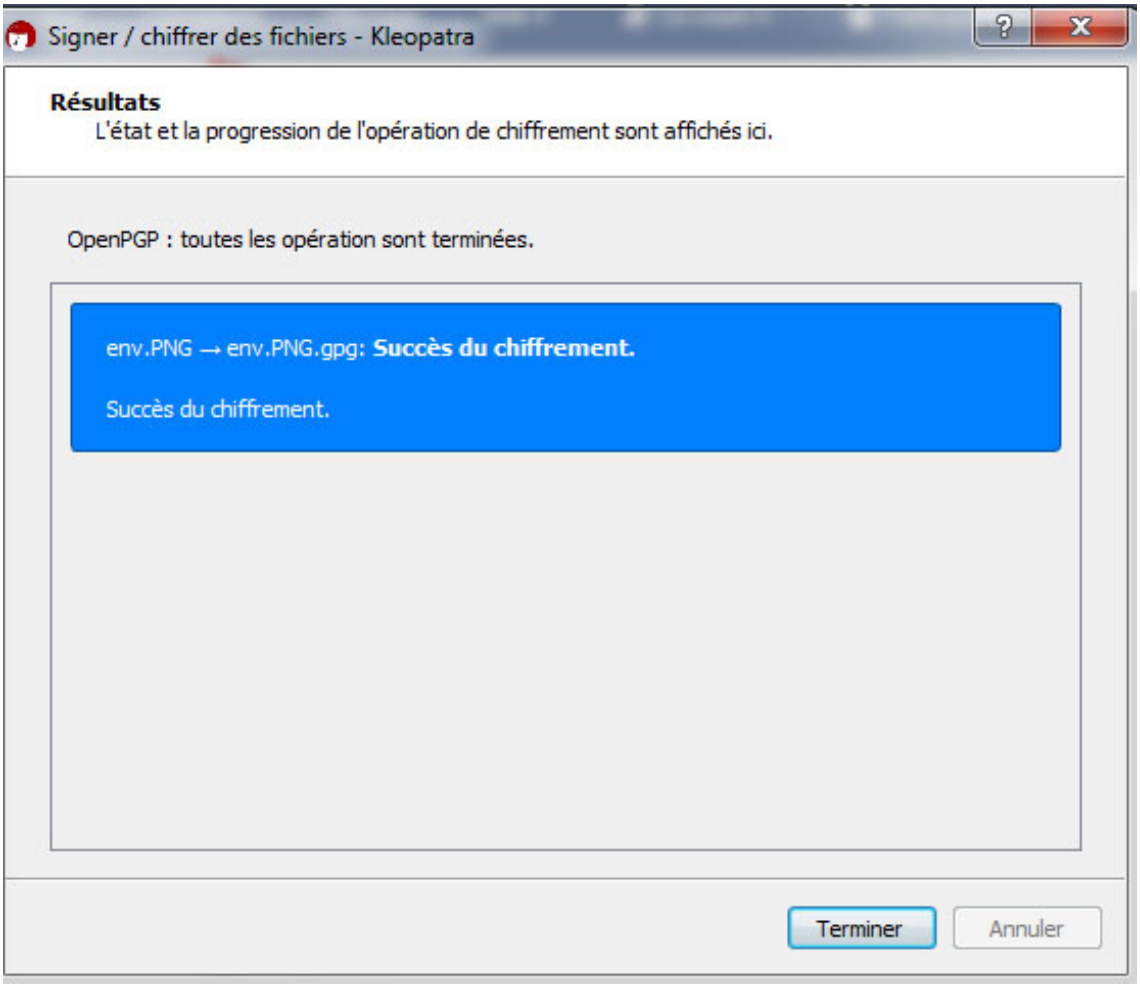
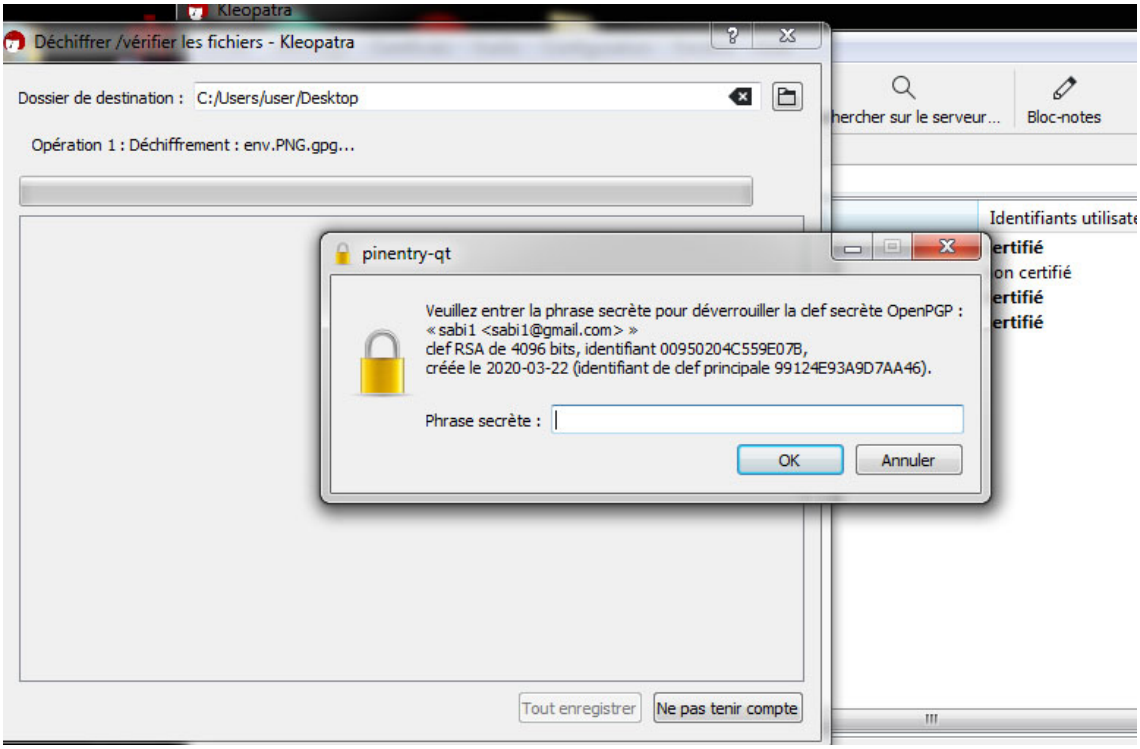


FIGURE 3.10 – Interface de chiffrement d'un fichier

3.3.11 Déchiffrer un fichier

Le destinataire déchiffre la pièce jointe reçu avec sa clé priveé .


Kleopatra
Déchiffrer /vérifier les fichiers - Kleopatra
Dossier de destination : C:/Users/user/Desktop
Opération 1 : Déchiffrement : env.PNG.gpg...
Tout enregistrer
Ne pas tenir compte
hercher sur le serveur...
Bloc-notes
Identifiants utilisat
ertifié
on certifié
ertifié
ertifié
pinentry-qt
Veuillez entrer la phrase secrète pour déverrouiller la clef secrète OpenPGP :
« sabi1 <sabi1@gmail.com> »
clef RSA de 4096 bits, identifiant 00950204C559E07B,
créée le 2020-03-22 (identifiant de clef principale 99124E93A9D7AA46).
Phrase secrète :
OK
Annuler

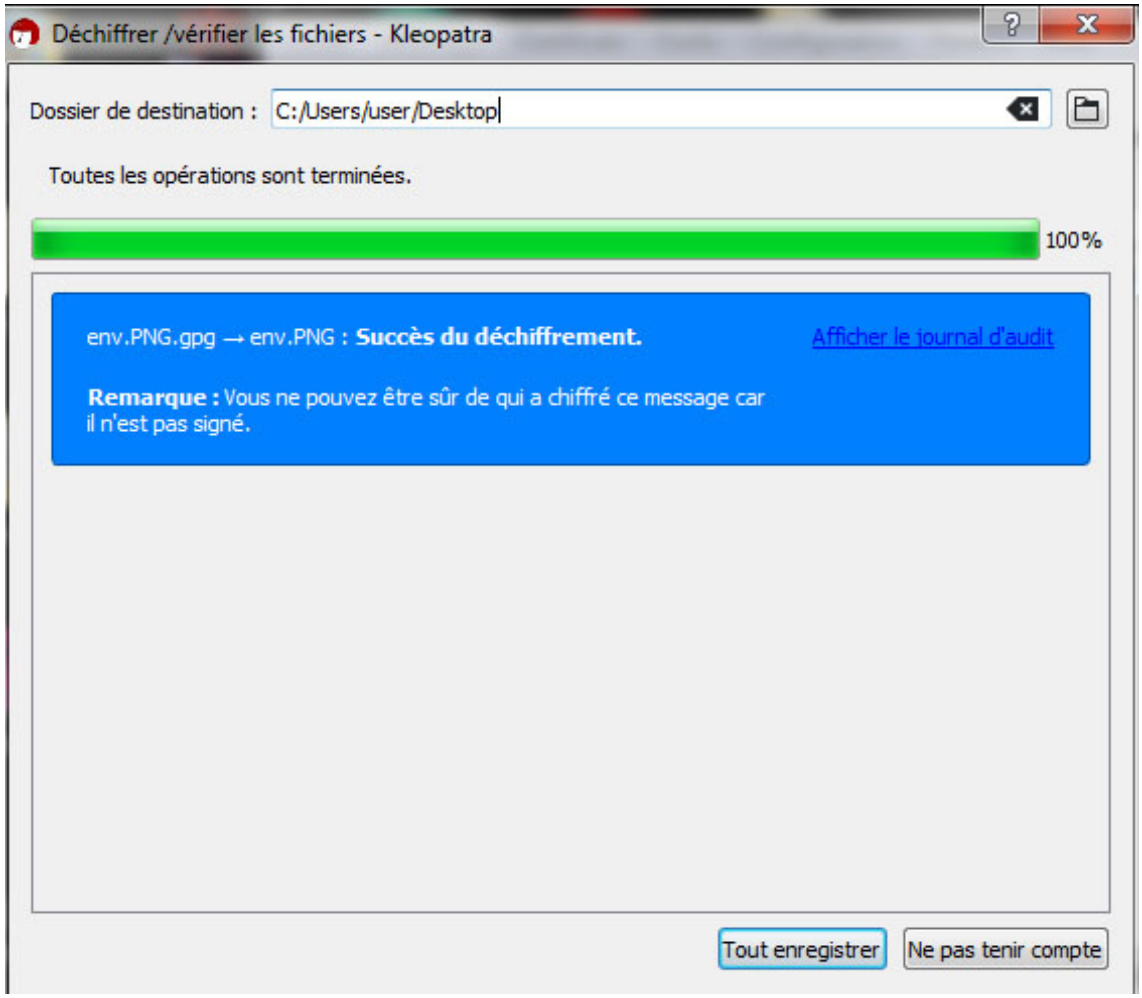


FIGURE 3.11 – Interface de déchiffrement d'un fichier

3.4 Scénario d'un cas d'utilisation :

il définie une suite logique des actions qui constituent ce cas. Le scénario suivant représente ce que fait l'acteur et ce que fait le système :

– Pour que l'utilisateur puisse accéder a la page d'accueil, il doit remplir le formulaire d'inscription qui contiens les champs suivant : nom, prénom, email, mot de passe et réponse a une question secrète, cette dernière est utilisée en

cas de perte de mot de passe pour accéder au compte, un message d'erreure est affiché si un champ est vide ou si l'adresse est invalide ;
- une fois le compte est crée, l'utilisateur va se connecter en tapent son email et son mot de passe, en cas d'erreur une fenêtre vas être affiché en indiquant que l'email ou le mot de passe est incorrect ;
- après l'authentification d'un utilisateur, la page d'accueil est affichée, l'utilisateur peut consulter et aussi mettre a jour son profil on modifiant les champs voulus ;
- L'utilisateur peut consulter les messages reçus et les messages envoyés, comme il peut envoyer des messages ;
- les messages échange entre utilisateurs sont sous forme d'une pièce jointe ;
- pour envoyer un message, il faut choisir une adresse de destination, saisir l'objet (facultatif), et aussi importer le message à envoyer (texte, image...etc) ;
- le chiffrement du message nécessite une clé privé, du cout l'utilisateur va accéder au logiciel kleopatra qui lui permet de généré une paire de clé ;
- pour la création de clés, l'utilisateur va saisir ces renseignements personnels, ensuit il vas entre une question secrète ;
- l'utilisateur exporte sa clé privé et sa clé public, céest avec cette dernirèr que les autres personne puisent lui envoyer des messages chiffrés,
- si une personne A veut envoyer un message a une personne B, elle doit écrire son message dans un fichier texte, une fois c'est fait elle importe la clé public de B sur kléopatra ensuit elle choisit le fichier a chiffre(le fichier peut être un pdf de taille limité, un fichier ou une image) ;
- la personne B reçoit le message chiffré, elle utilise sa propre clé (sa clé privée)pour le déchiffrer.

3.5 Conclusion

A travers ce chapitre, nous avons cité les diffŕentes outils de dévloppement de notre système et quelques interfaces graphiques que nous avons jugé les plus impor-

tantes. Cette étape nous a permis de réaliser notre objectif qui consiste à réalise un système de messagerie sécurisée sur une plateforme web .

Conclusion et perspectives

Dans ce travail, nous avons réalisé un système de messagerie sécurisé, ce system permet d'assuré l'authentification, la confidentialité, et l'intégrité.

Notre objectif était d'étudier d'abord les aspects théoriques qui entourent un environnement de messagerie comme les protocoles utilisés, l'architecture logicielle, la sécurité informatique, et enfin étudier l'utilisation et les mécanismes de fonctionnement.

Ensuite, nous avons entamé la seconde partie dans laquelle nous avons identifié les différents acteurs interagissant avec le système réalisé. Aprè s cela, nous avons réalisé la modélisation fonctionnelle. En effet, nous avons décrit les besoins des acteurs, suivi de la spécification des besoins fonctionnels Ã travers les diagrammes de cas d'utilisation et de l'analyse des besoins en utilisant les diagrammes de séquence. Enfin, dans la dernière partie du projet, nous avons réalisé notre travail en spécifiant les outils de développement de l'application et les langages de programmation utilisés, suivi d'un aperçu sur les interfaces que comprend celui-ci.

A l'avenir, nous souhaitons ajouter un espace de partage des médias tels que les vidéos, la communication en groupe ainsi mettre en Å“uvre l'envoi de données de types data et voix.

Bibliographie

[1] https://www.certeurope.fr/blog/guide-certificat-x509/, (Consulté le 10/01/2019).

[2] http://www.authsecu.com, (Consulté le 10/01/2019).

[3] http://www.la-mise-en-page.com/2019/02/14/quels-sont-les-differents-types-de-messageries-electroniques/, (Consulté le 10/01/2019).

[4] https://www.mixconcept.fr/blog/messagerie-professionnelle-9-raisons-dutiliser-out (Consulté le 10/01/2019).

[5] https://www.letsrockbusiness.com/messagerie-pro-gmail/, (Consulté le 10/01/2019).

[6] https://commentarticle.ru/internet/sites-populaires/yahoo/19399-quels-sont-les-avantages-de-yahoo.html, (Consulté le 10/01/2019).

[7] https://www.igm-univ-mlv.fr, (Consulté le 10/10/2019).

[8] https://app.mailjet.com/support/qu-est-ce-que-le-ssl-et-le-tls-est-ce-que-cela-s 32.htm, (Consulté le 15/02/2019).

[9] http://www.tutorialspoint.com/internet_technologies/e_mail_protocols.htmCopyrighttutorialspoint.com, (Consulté le 18/03/2019).

[10] https://www.sites.univ-rennes2.fr/urfist/messagerie_electronique_fonctionnement, (Consulté le 20/10/2019).

[11] https://www.memoireonline.com/11/13/7773/m_Conception-et-developpement-d-une-application-mobile-de-vente-flash-sous-android.html, (Consulté le 2/02/2020).

[12] http:/www.ibm.com, (Consulté le 28/11/2019).

[13] https://www.wearecom.fr/dictionnaire/arpanet/, (Consulté le 4/02/2020).

[14] https://siguillaume.developpez.com/tutoriels/linux/mise-place-systeme-messagerie-electronique-sous-linux, (Consulté le 9/02/2020).

[15] A.Douiri. Etude et développement d'une application de messagerie électronique. Mémoire master, Ecole Nationale des Sciences de l'informatique, TUNIS, 2010.

[16] A.RAISSI. conception et développement d'un site web de e-commerce pour le compte de lsat nokia. Mémoire master, Université virtuelle, TUNIS, 2012/2013.

[17] A.SIDER. Chapitre 5 : « service de messagerie internet et protocoles associés ». http://www.univ-bejaia.dz, (Consulté le 1/10/2019).

[18] B.Cousin. «le système de messagerie d'internet ». http://www.people.irisa.fr/Bernard.Cousin/Cours/messagerie.2p.pdf, (Consulté le 1/10/2019).

[19] B.Merad and M.Zidane. mise en place d'un serveur de messagerie eléctronique interne avec hmailserver au sein de l"epb. Mémoire master informatique, Université Abderrahmane Mira, Béjaia-Algerie, 2017.

[20] C.MORLY, J. HUNGUES, and B. BERLAND. *UML pour l'analyse d'un système d'information*. Dunod, 2002/2006.

[21] D. Gaba and J. Gabay. *UML2 Analyse et conception*. DUNOD, 2008.

[22] G.Solange. *Sécurité informatique et réseaux*. Malakoff : Dunod, 2016.

[23] H.AYADI and F.ASLI. Conception et réalisation d'un système de messagerie électronique. Mémoire licence informatique, Université Abderrahmane Mira a revoiiiiir, Béjaia-Algerie, 2011.

[24] I.Jacobson, G.Booch, and J.Rumbaugh. *Le processus unifié de développement logiciel*. Eyrolles, 2000.

[25] K.Bourdache and S.Ouali. conception et réalisation d'un système de messagerie électronque en intranet. Mémoire master informatique, Université Abderrahmane Mira, Béjaia-Algerie, 2016.

[26] L.Audibert. Uml 2. *Institut Universitaire de Technologie de Villetaneuse– Département Informatique*, 2007.

[27] P.Roques and F.Vallée. *UML en action : de l'analyse des besoins à la conception.* Editions Eyrolles, 2003.

[28] P.Roquesl. *UML 2 : Modéliser une application web.* Editions Eyrolles, 2008.

[29] C. Soutou. *UML2 pour les bases de données.* EYROLLES, 2006.

RÉSUMÉ

Le courrier électronique est l'un des moyens de communication les plus utilisés. Comme les informations échangées soient toujours sujets à des attaques, la sécurité informatique doit être assurée. Dans ce travail, nous avons réalisé un système de messagerie sécurisé. Ce système permet la transmission des messages chiffré. Pour un émetteur, le message envoyé est chiffré par la clé publique de destinataire, le récepteur déchiffre le message avec sa clé privé. Cet échange sera fait une fois que l'émetteur et le récepteur sont authentifiés. En conséquence, la confidentialité, l'intégrité des donnés et l'authentification sont assurées.

Mots clés : système de messagerie, courrier électronique, sécurité informatique, chiffrement, déchiffrement.

ABSTRACT

Email is one of the most widely used means of communication. As the information exchanged is always subject to attacks, IT security must be ensured. In this work, we have achieved a secure messaging system. This system allows the transmission of encrypted messages. For a sender, the message sent is encrypted by the recipient's public key, the recipient decrypts the message with his private key. This exchange will be done once the sender and receiver are authenticated. As a result, confidentiality, integrity and authentication are ensured.

Key words : messaging system, electronic mail, computer security, encryption, decryption.