Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saâd Dahlab, Blida
USDB.
Faculté des sciences.
Département informatique.

Mémoire pour l'obtention du Diplôme de Master en Informatique

Option : Ingénierie de logiciel

Sujet :

Conception et réalisation d'un site web d'enchère en ligne sécurisé

Organisme d'accueil :
Algérie Telecom Djaweb

Réalisé par :

BATEL Sarra **CHANANE Aicha**

Suivie par :

Mr SIDOUMOU

Promotion : 2010/2011

Remerciement.

Tout d'abord on tient à remercier notre DIEU le tout miséricordieux de nous avoir permis d'achever ce travail.

Nous remercions nos parents pour leur soutient morale, leur disponibilité, leur compréhension et surtout leur encouragement

Nous adressons nos vifs remerciements à Mr SIDOUMOU, notre promoteur, pour ses conseils, sa collaboration et ses encouragements

Nous remercions notamment Mme GHEDAB Nassima notre encadreur à Algérie Tecom djaweb,Mr SAYAH Mustapha , et tous nos chers enseignants pour leur effort durant les 5 années d'étude

Nous remercions nos ami(e) surtout Krimou, Mohamed et Dalila pour leurs conseils et leurs aide.

Enfin, nous remercions toute personne ayant contribuée de prés ou de loin à la progression de ce projet.

Dédicace

Je dédie ce modeste travail

À mes très chers parents que nul remerciement ne peut leur rendre une goute de leurs sacrifices, leurs bienveillances et leur compréhension tout au long de ma vie, j'espère de tout mon cœur que j'ai réussi à réaliser leur rêve de me voir réussir dans mes études.

À mes grands parents à qui je dois tout l'amour et le respect, que dieu les garde pour nous.

À mes sœurs « «IKRAM et AMIRA », mes frères « AYOUB et FAYCAL », mes tantes, mes oncles, mes cousins, mes amis et toute personne qui fait parti de mon entourage.

Une dédicace très spéciale à mon français ABDENOUR et à toute sa famille.

Et a toutes personnes qui m'ont aidée de prés ou De loin.

Aicha

Dédicace

Je dédie mon travail

À la plus chère et la plus précieuse perle qui existe sur la terre, a celle que je ne pourrai jamais lui rendre ses bienveillances tout au long de ma vie « ma mère »

A mon cher père qui n'a jamais cessé de m'aider et de m'encourager durant tout mon parcours

Que dieu le tout puissant vous garde mes chers parents

À mon frère jumeau Amine, mes sœur imene et nesrine, mon frère mahdi, mes cousins, cousines, et tout ma famille

À ma chère tante « Zakia » que j'aime bien et qui souhaite me voir réussir dans mes études et dans ma vie, que dieu la garde pour nous.

A tous mes ami(e) et toute personne qui fait parti de mon entourage.

Sarra

RESUME

L'innovation technologique, aujourd'hui, change nos habitudes. L'Internet a franchit les limites spatio-temporelles. On n'a plus besoin de se déplacer pour acheter ou vendre des produits. L'une des technologies née d'Internet est le e-commerce. Une sous catégorie du e-commerce est l'enchère en ligne.

Les plateformes de e-Commerce, sur lesquelles portera notre application, sont les plateformes de vente et d'achat aux enchères Vickrey.

Cependant, les communications via le réseau Internet ne sont pas à l'abri d'attaques visant à intercepter les informations confidentielles, d'usurper l'identité d'un utilisateur ou d'injecter de fausses informations. Tous ces problèmes risquent de freiner le développement de ce type de e-commerce.

L'objectif de notre travail est de faire face à ces attaques et offrir un environnement sûr aux clients en assurant leurs authentifications, la confidentialité et l'intégrité des données échangées.

Le protocole SSL/TLS et la signature digitale, des technologies basées sur la cryptographie à clé publique, seront nos solutions contre ces attaques.

Mots clés : les enchères, enchère vickrey, e-commerce, sécurité web, cryptographie à clé publique (asymétrique), signature digitale, SSL/TLS.

ABSTRACT

Today technological innovation changed our habits. The Internet has crossed the limits of space and time. There is no more need to move to buy or sell products One of the internet technology is e-commerce, one of ecommerce's sub categories is Auction on line.

The e-Commerce platforms on which will cover our application, are the most widespread platforms for the purchase and sale by vickery' auction,

However, the communications on the Internet are not immune to attacks designed to intercept confidential information, to usurp the identity of a user or to inject false information, All these problems may hinder the development of this e-commerce 'type.

Our work and aims to cope with these attacks and provide a safe environment for the clients by ensuring their authentications, the confidentiality and integrity of the data exchanged.

The SSL/TLS protocol and Digital signature, technologies based on the asymmetric cryptography will be our solutions against these attacks.

Key words: auctions, vickrey auction, e-commerce, web security, asymmetric cryptography, digital signature,SSL/TLS.

Sommaire

Liste des figures

Liste des tableaux

Introduction

1. Problématique et objectifs

La communication, l'échange et le partager d'information sont devenu nécessaire depuis l'arrivée d'Internet et l'essor des nouvelles technologies associées. L'innovation de ces technologies d'information et de communication à favoriser l'émergence d'applications de plus en plus complexe telle que les multimédias et le commerce électronique.

Le commerce électronique est la combinaison des pratiques commerciales traditionnelles avec l'ordinateur et les technologies d'information, et des communications. Le commerce électronique n'est pas inédit. Il a vu le jour dans les années 60 sur des réseaux privés, à l'époque ou de grandes organisations ont mis sur pied des installations d'échange de données informatisées. De nos jours, le commerce électronique n'est plus l'apanage des grandes entreprises et des réseaux privés.

Les applications de e-commerce suivent généralement le modèle qui comporte les phases suivantes:

- Identification des besoins.
- Recherche des meilleures offres.
- Négociation.
- Achat.
- Livraison du produit.

La phase de négociation porte sur l'amélioration des conditions de vente et ce sont les protocoles d'enchères qui offrent les mécanismes les plus compétitifs pour la négociation.

Les enchères sont l'une des formes de négociation les plus répandues dans le e-commerce. Les enchères en ligne offrent la possibilité de participer ou d'en créer sans se déplacer physiquement, ce qui augmente le nombre de participants de manière considérable, avec un gain d'espace et de temps, contrairement à la méthode classique où il fallait la présence sur place de tous les participants. Les enchères sont devenues un mode d'achat et de vente de plus en plus répandu. Ainsi les ventes aux enchères concernent des biens ou des services de plus en plus complexes comme des concessions pétrolières, et des biens ayant une valeur de plus en plus grande.

Une enchère comporte les acteurs suivants :

- **Un initiateur** « commissaire priseur » : qui propose un produit avec un prix de base.
- **Des participants** « enchérisseurs » : qui font leurs offres selon un protocole bien définit.

À la fin, l'un d'entre eux emportera l'enchère.

Il existe deux types d'enchère, l'un où les offres des enchérisseurs sont cachées, comme l'enchère Vickrey où chaque participant soumet une offre sans connaitre les offres des autres, et elle se fait en un seul tour. Le participant qui a fait l'offre la plus grande gagne mais il doit payer le prix de la deuxième plus grande offre. Le problème qui se pose est que l'initiateur de l'enchère peut la falsifier ou bien ajouter une nouvelle fausse offre sans que les participants ne se rendent compte. Ainsi Celui qui remportera l'enchère risque de payer plus qu'il en faut, donc ces transactions de ventes aux enchères ne sont pas à l'abri des falsifications.

Dans ce contexte née notre problématique :

Comment mettre les transactions d'enchères vickrey, actuellement largement utilisées, a l'abri des falsifications.

Un tas de questions auxquelles nous allons répondre pour atteindre les objectifs tracés pour savoir garantir l'authentification des utilisateurs , la confidentialité et l'intégrité des échanges afin d'offrir plus de transparence pour les internautes.

Pour la réalisation de notre application, une étude bibliographique portera sur le commerce électronique et les enchères, la sécurité des échanges sur Internet ainsi qu'une étude sur le protocole de sécurité SSL. Nous passerons ensuite à la conception puis la réalisation de notre système qui consiste à réaliser un site web d'enchère en ligne sécurisé.

2. Structure du mémoire :

Notre travail est organisé comme suit :

Partie 1 : Etat de l'art où une étude bibliographique parcourant les notions abordées au long du projet. Elle englobe deux chapitres :

Chapitre 1 : dans lequel nous présenterons le e-Commerce, le e-Commerce en Algérie, les cause qui le retardant en Algérie, et les solutions proposer pour un futur déploiement .Puis nous exposons les différents protocoles d'enchères.

Chapitre 2 : portera sur la sécurité web. Nous aborderons les notions fondamentales sur la cryptographie et les protocoles d'échanges sécurisés.

Partie 2 : Conception et réalisation qui comprend les deux chapitres suivants :

Chapitre 3 : Cette partie décrit et délimite les parties à développer. En premier lieu une modélisation UML détaillée décrit notre système.

Chapitre 4: Réalisation dans lequel nous présenterons l'architecture technique de notre système avec justification de nos choix en matière d'environnement et de développement (serveurs, langage, etc.). Une présentation détaillée du fonctionnement de notre système.

Nous terminerons par une conclusion générale, quelques perspectives et des annexes. Nous présentons dans la première annexe quelques algorithmes à clé publique. Et une dernière annexe sur le langage de modélisation UML.

CHAPITRE 1

LE COMMERCE ELECTRONIQUE ET LES ENCHERES

1. Profil Global de la Société Algérie Télécom-Pole Djaweb Services :

1.1- Historique :

AT-Pole Djaweb Services, est une société par actions à capitaux publics opérant sur le marché des réseaux et services Internet.

Le Pole Djaweb Services offre une gamme complète de produits et services (Internet, voix et data) sur mesure.
Particuliers, professionnels et entreprises trouvent dans la gamme de nos produits une panoplie d'offres répondant à leurs attentes, facilitant leurs besoins de communication et augmentant la performance de leurs activités.

1.2- La Mission de AT-Pole Djaweb:

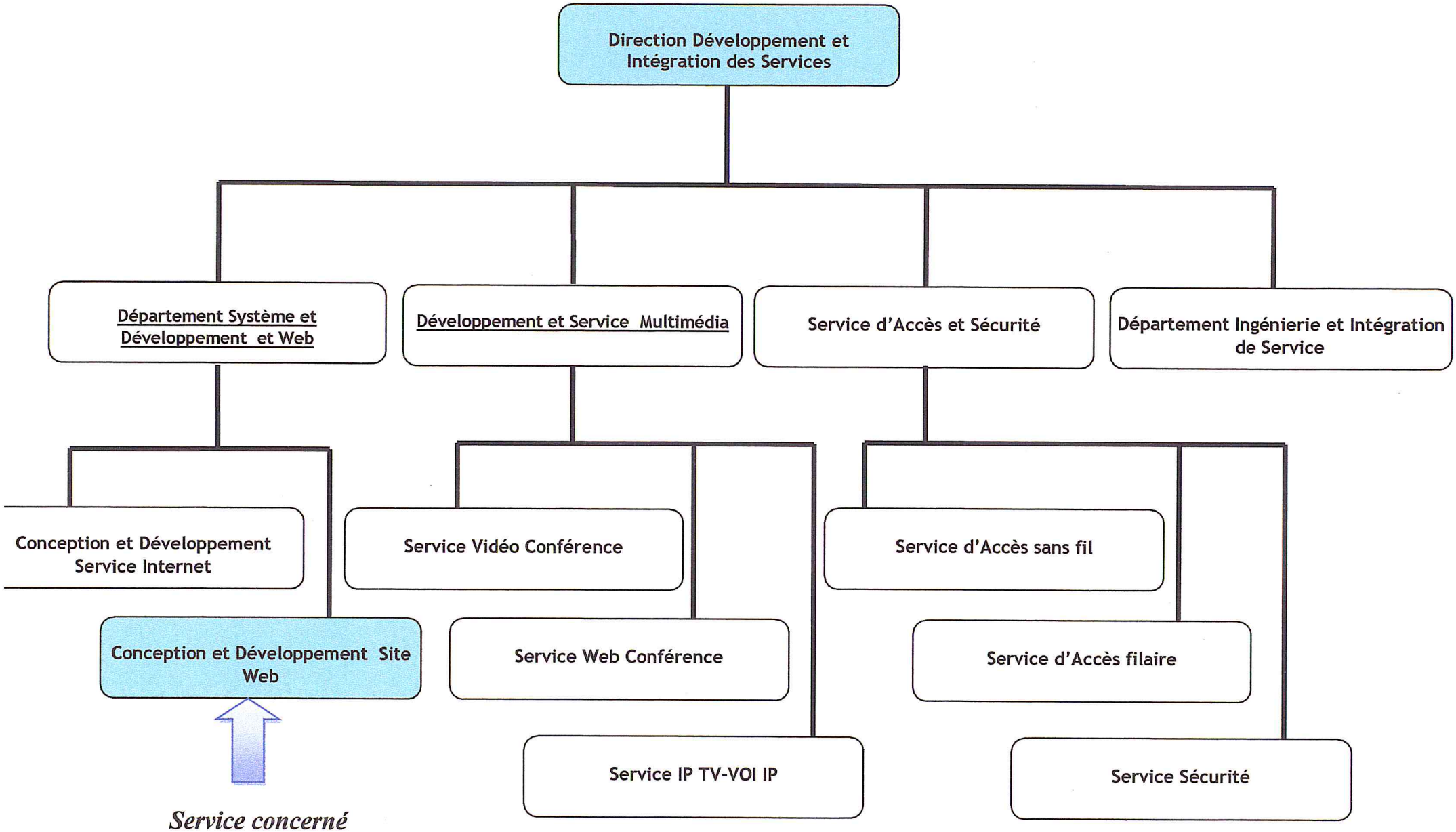
La mission d'AT-PDS est de mettre son expertise, sa capacité au service de l'innovation et la passion qui l'anime au service des projets, des ambitions et de la créativité de ses clients, afin de faire de la technologie leur meilleure alliée dans l'expression de leur potentiel.

Ils sont déterminés à

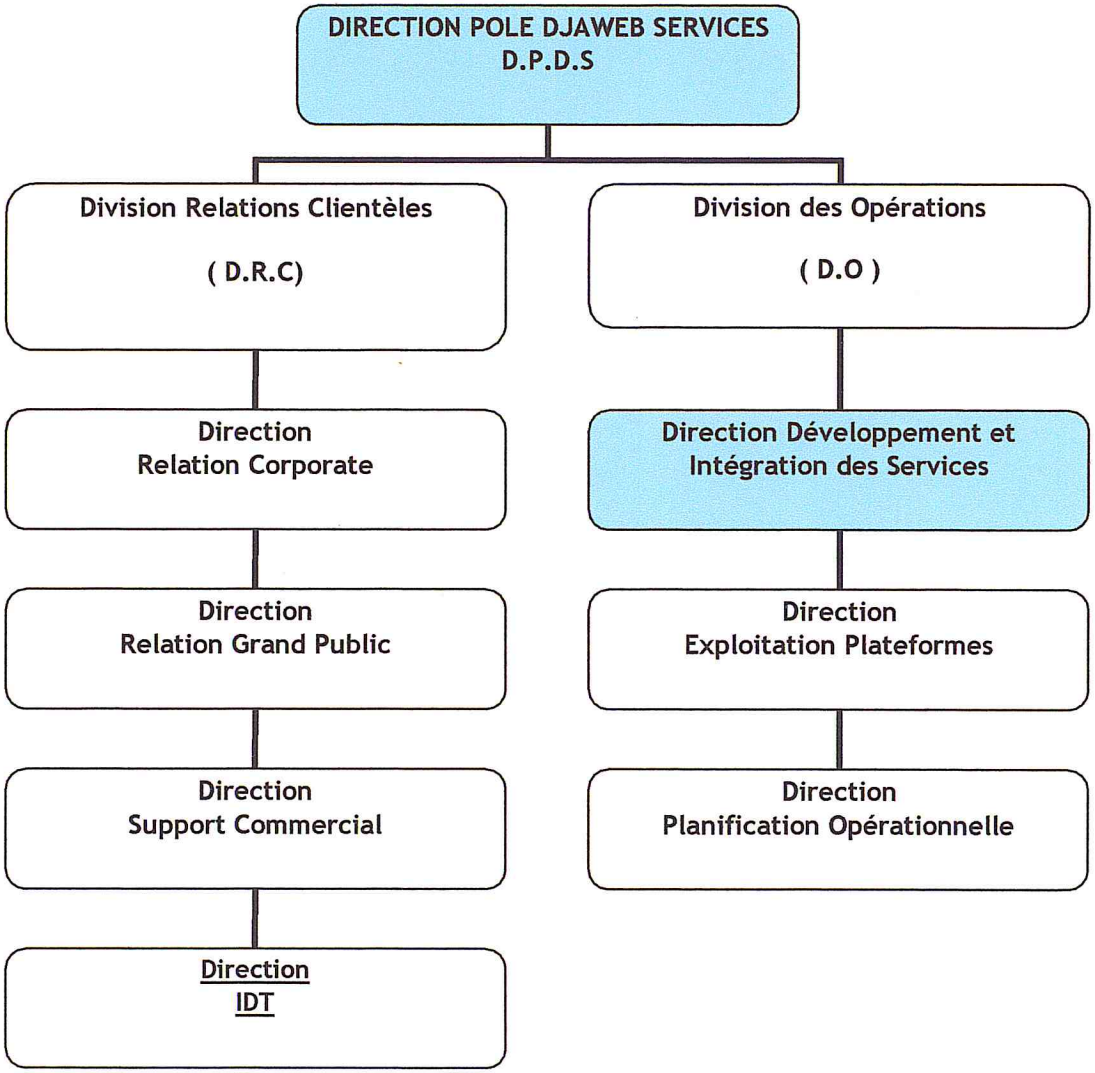
- Participer au développement de la société de l'information en mettant en place une plate forme Internet de grande capacité ;
- Promouvoir l'Internet en Algérie en multipliant le nombre d'accès, en augmentant l'accessibilité et ce, en diversifiant les points de présence au niveau de toutes les wilayas du territoire national et en réduisant les coûts d'abonnement ;
- Développer les nouveaux services liés à l'Internet tel que le e-commerce, la vidéo conférence, la voix sur IP, l'audio vidéo streaming, l'Internet mobile etc…
- Assurer la formation dans le domaine des nouvelles technologies de l'information en général, et dans les télécommunications et l'informatique en particulier.

Et dans le chapitre qui suit nous allons présenter le e-commerce et les enchères

ORGANIGRAMME GENERALE DE LA DIRECTION DE DEVELOPPEMENT ET INTEGRATION DES SERVICES :



ORGANIGRAMME DE LA DIRECTION POLE DJAWEB SERVICES



PARTIE 1

ETAT DE L'ART

Le e-Commerce

1. Introduction

Le e-commerce est une technologie de plus en plus utilisée. Elle offre beaucoup de possibilités telles que la recherche rapide et à moindre coût, la délocalisation des participants, un marché bien plus large.

Initialement le e-commerce était vu comme une requête envoyée par l'utilisateur via une page web pour acheter, vendre ou rechercher un produit.

Le commerce électronique peut être défini comme l'ensemble des échanges électroniques liés aux activités commerciales. Il recouvre toute opération de vente de biens et de services via un canal électronique.

2- Le monde et le e-commerce

Le commerce électronique consiste à faire des achats et des ventes en utilisant Internet. La façon d'y accéder ou les appareils utilisés n'ont pas une grande influence. On peut faire du e-commerce avec un PC et une ligne ADSL.

Beaucoup d'opportunités peuvent s'offrir avec l'arrivé du e-commerce telles que les chaines logistiques, les publicités sur internet, les marchés électroniques, les services à distance, l'échange de données et les transactions en ligne.

3. Définition

Parmi les définitions du e-commerce on a :

"Le commerce électronique couvre toute transaction d'affaire ou administrative ou échange d'informations en utilisant des techniques de la technologie d'informations" **[1]**.

Les deux types de transactions les plus utilisées sont **[1]**:

- Le B2B e-commerce : business to business, e-commerce couvre toute transaction où le vendeur et le client sont des entreprises ou des organisations commerciales.
- Le B2C e-commerce : Business to client, e-commerce couvre toute transaction où le vendeur est une compagnie et le client un consommateur.

Les autres types de transactions sont:

- Le C2C (consumer to consumer).
- Le C2B (consumer tu business).
- Le e-commerce pour un but non commercial (université, gouvernement, organisation charitable, etc.)

4. Le E-Commerce En Algérie :

L'Algérie est un pays émergent où les nouvelles technologies peuvent avoir un grand impact sur l'économie nationale. Le e-commerce est l'une de ces technologies. Si dans les pays développés l'utilisation du e-commerce est assez démocratisée, en Algérie l'adoption de cette technologie a encore du chemin devant. L'Algérie s'apprête à intégrer l'organisation mondiale du commerce et pour que nos entreprises puissent rivaliser avec celles des pays développés, elles doivent utiliser tous les moyens techniques possibles ; le e-commerce est l'un de ces moyens et qui possède une part assez importante du marché mondial. L'Algérie doit faire face à beaucoup de problèmes avant d'adopter le e-commerce.

La diffusion du e-commerce peut prendre différents chemins selon le pays. Le chemin à prendre peut dépendre de plusieurs paramètres comme les lois du pays, les infrastructures de télécommunications, la diffusion d'internet et la culture.

4.1. Les différents facteurs retardant le e-Commerce en Algérie

On peut tirer quelques axes qui ont une influence significative sur le retard de développement du e-commerce en Algérie. Ces axes sont [1]:

a- Le e-Banking en Algérie

L'e-banking est quasiment inexistant en Algérie. Quelques banques publiques possèdent des sites web mais aucune allusion aux transactions en lignes. Quelques banques étrangères proposent ce genre de solution, mais très peu d'Algériens possèdent des comptes. Il existe en Algérie une particularité qui est que la majorité des habitants possèdent des comptes ccp (comptes postaux) alors que la poste n'est pas considérer comme une banque. La poste algérienne propose différents services comme le transfert d'argents mais aucun ne peut se faire en ligne. Le seul service proposé en ligne est la vérification du solde. Cependant, le serveur hébergeant ce

service est souvent hors service. Le système bancaire algérien est en retard il n'est pas favorable au développement du e-commerce.

A cause de la quasi-inexistence de l'e-payement, les seules applications possibles en Algérie sont la consultation d'annonces via Internet. Ensuite, le paiement se fait par cash et la livraison se fait de main en main.

b- L'infrastructure Telecom

Depuis la démocratisation du marché du téléphone mobile en Algérie, la majorité de la population est en mesure de s'en procurer, les tarifs sont assez abordables. Le marché du mobile est partagé par trois opérateurs concurrents. Cependant, le monopole d'Algérie télécom sur Internet est toujours présent bien qu'il existe quelques opérateurs privés mais qui sont à la merci d'Algérie Telecom. Le manque de concurrence a impliqué un réseau et une connexion Internet relativement lente. Quant au prix, il demeure assez abordable. Même en absence de concurrence, Algérie Telecom œuvre à démocratiser Internet mais la qualité du service demeure relativement moyenne et souvent avec une saturation des lignes.

c- Législations et protection du consommateur

Il n'existe aucune législation qui s'applique au e-commerce car ce type de transactions est presque inexistant et la loi appliquée est la loi judiciaire classique.

d- La confiance

Les Algériens ont l'habitude de bien examiner les produits avant d'acheter car la contrefaçon est très répandue et une future plateforme du e-commerce doit pouvoir mettre en évidence la confiance.

e- Internet dans les écoles et universités

Les universités algériennes sont dotées d'un réseau intranet et d'une connexion Internet, mais seuls les chercheurs et les enseignants ont accès ; les étudiants en cycle de graduation ne peuvent avoir accès au sein de l'université sauf pour des cas particuliers rares.

4.2. Solutions pour le déploiement du e-commerce en Algérie

- le développement de l'infrastructure des télécommunications.
- La présence d'un système du e-banking fiable, sécurisé et capable de prendre en charge les transactions du e-commerce.
- Une législation pour protéger les consommateurs et les vendeurs adaptée au e-commerce.
- Une législation adaptée aux transactions de type e-commerce.
- Un prix d'utilisation d'Internet adapté au revenu moyen des citoyens.
- Un système de e-commerce est capable d'inspirer la confiance dans un environnement où la crainte et la fraude sont courantes.
- L'élimination de l'analphabétisme (Ordinateurs et Internet) en facilitant l'accès à ces technologies dans les écoles, universités et endroits publiques.
- Le contenu en langues locales peut aider au développement d'Internet.
- L'adoption et la promotion du e-business par les sociétés.

Dans ce qui suit nous allons aborder les différents protocoles d'enchères, suivie d' une comparaison entre eux.

Les Enchères

1. Historique

Les enchères sont des mécanismes d'allocation de ressources rares dont l'utilisation remonte à l'antiquité. On reconnaît généralement que l'histoire des enchères a débuté vers 500 av. J.-C.Dans ces écrits, Hérodote décrit des enchères au premier prix aux cours desquelles la main des jeunes femmes était accordée au plus offrant (vente d'esclave aux enchères).

Dans les sociétés contemporaines, les mécanismes de vente aux enchères ont été traditionnellement utilisés pour les produits de l'agriculture et de l'élevage. Parallèlement, les objets pour lesquels il est difficile d'estimer les coûts de production et ceux pour lesquels les coûts ne reflètent pas la valeur font également l'objet de ventes aux enchères (comme c'est le cas pour les objets et œuvres d'art).

Plus récemment, les enchères sont devenues un mode d'achat et de vente de plus en plus répandu. Ainsi les ventes aux enchères concernant des biens ou des services de plus en plus complexes comme des concessions pétrolières, des licences de téléphonie mobile ou encore des fréquences radio et des biens ayant une valeur de plus en plus grande.

Finalement, Internet a permis de rendre plus accessible ce mode d'achat et d'étendre considérablement la diversité des produits mis en vente. Ces sites internet permettent aux utilisateurs inscrits de vendre ou d'acheter des biens d'une grande diversité, qu'ils soient neufs ou usagés.

2. Définition

Les enchères sont l'une des formes de négociation les plus répandues dans le e-commerce **[5]**. Les enchères en ligne offrent la possibilité de participer ou d'en créer sans se déplacer physiquement, ce qui augmente le nombre de participants de manière considérable, avec un gain d'espace et de temps. Une enchère commence par une personne qui est son initiateur et qui propose un produit et les autres participants sont des enchérisseurs qui font leurs offres selon un protocole bien

définit. À la fin, l'un d'entre eux emportera l'enchère. L'utilisation des agents dans les enchères fait que chaque agent représente un participant et décide quand participer ou lancer une offre, analyse le marché et essaie de faire les meilleures affaires, l'agent doit connaître la valeur de l'objet a enchérir et ne doit pas payer plus que cette valeur, mais la valeur peut être différente d'un utilisateur à l'autre. Supposons qu'une voiture soit mise à l'enchère et que cette voiture a été conduite par un champion de course, pour certains la valeur de cette voiture pourrait être de 1000.000 Da mais pour des fans, la valeur pourrait être beaucoup plus grande, ce qui est une valeur privée ; donc dans une enchère, un agent doit pouvoir bien représenter son propriétaire et connaître la vraie valeur des produits pour son propriétaire.

Il y a beaucoup de types d'enchères, mais il y en a 4 qui sont très répandus, il y a qui se déroulent en un tour ou en plusieurs tours. Les 4 types d'enchères que nous distinguons sont:

a) Enchère anglaise (premier-prix offre-publique)

L'initiateur commence l'enchère, d'habitude, par l'annonce d'un prix de réservation (le prix minimal pour lequel il est d'accord pour vendre l'objet). Chaque participant annonce publiquement son offre, en plusieurs tours successifs. Quand aucun participant ne veut plus augmenter son offre, l'enchère s'arrête et le participant ayant fait la plus grande offre gagne l'objet au prix de son offre. **[6]**.

b) Enchère Hollandaise (descendante)

L'initiateur commence par proposer un prix et par des tours successifs, diminue ce prix jusqu'au moment où un des participants achète l'objet au prix proposé. **[6]**.

c) Enchère première offre-cachée

L'initiateur commence l'enchère et chaque participant soumet une offre, dans un tour unique, sans savoir les offres des autres. Le participant qui a fait la plus grande offre gagne l'objet et paye le montant de son offre **[6]**.

d) Enchère Vickery (deuxième-prix offre-cachée)

Chaque participant soumet une offre sans connaitre les offres des autres, en un seul tour. Jusqu'à maintenant, le protocole est le même que celui de l'enchère premier-prix

offre-cachée. La différence est que le participant qui a fait l'offre la plus grande gagne mais il doit payer le prix de la deuxième plus grande offre.
L'enchère Vickery est moins répandue dans les enchères entre humains à cause du fait que l'initiateur peut mentir sur le deuxième prix élevé et faire payer le gagnant plus que ce prix. Dans les enchères électroniques on peut régler ce problème en imposant une signature digitale à toutes les offres des participants, de cette manière, on peut avoir une possibilité de vérifier le prix à payer [6].dans ce présent projet on propose de gérer ca en utilisant la signature digitale.

3. Comparaison entre les 4 protocoles

Protocol/élément	Détermination du gagnant	Le processus	Type d'enchère
Anglaise	Premier prix	Ouverte à la criée	ascendante
Hollandaise	Descendre graduellement le prix Jusqu'à ce que l'un des enchérisseurs dise le plus grande offre	Ouverte à la criée	descendante
Première offre cachée	Le bien est alloué à l'agent qui fait la plus élevée des offres; le gagnant paye l'offre la plus élevée.	Enchère à un seul tour	Les enchérisseurs soumettent une offre secrète du type « enveloppe cachetée »
Vickery	A mise secrète du type second prix	Le bien est alloué à l'agent qui fait la plus élevée des offres;	Le gagnant paye la 2nd plus haute offre;

Tableau I.1

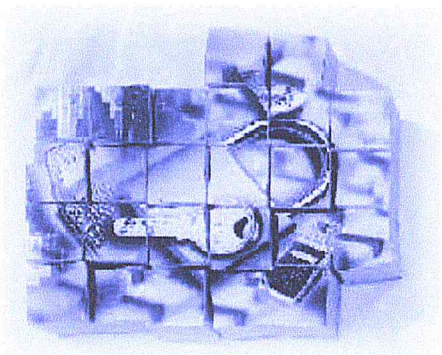
Conclusion

Le passage au commerce électronique constitue un vrai moteur de relance pour l'économie algérienne. Son introduction devient de plus en plus nécessaire et urgente vu la situation commerciale hyper développée dans le monde. Son implantation va permettre a nos entreprises de s'engager dans le marché internationale.

Dans ce présent projet notre travail consiste a élaboré un site e-Commerce d'enchère en ligne sécurisé en utilisant le protocole d'enchère vickery. L'analyse du protocole d'enchère vickrey nous a aidés à déduire leurs besoins en sécurité. La réponse à ces besoins est l'objet du chapitre suivant.

CHAPITRE 2

LA SECURITE WEB



« Le seule système infaillible est celui qui est éteint et débranché,
enfermé dans un coffre en titane, enterré dans un block en béton,
entouré d'un nuage de gaz neuroplégique et de garde armé très bien payés.
Même ainsi je ne parierais pas ma vie dessus »

Jim Conallen.

1. Introduction

Depuis quelques années, la révolution des moyens de communication, particulièrement l'Internet a mené à une large liberté en circulation d'informations et une haute disponibilité de nombreuses ressources. Ceci a fait naître de nouveaux problèmes dans la sécurité informatique donc de nouveaux besoins.

La sécurité web, une branche de la sécurité informatique , c' est l'ensemble des techniques qui visent la préservation de la confidentialité et l'intégrité des données échangées via Internet.

Nous présenterons dans ce chapitre les concepts de base de la cryptographie. Les méthodes de cryptage symétrique, asymétrique, le hachage et la signature numérique.

Nous présenterons ensuite quelques protocoles de sécurité tels que SLL/TLS, le protocole de sécurisation des transactions web.

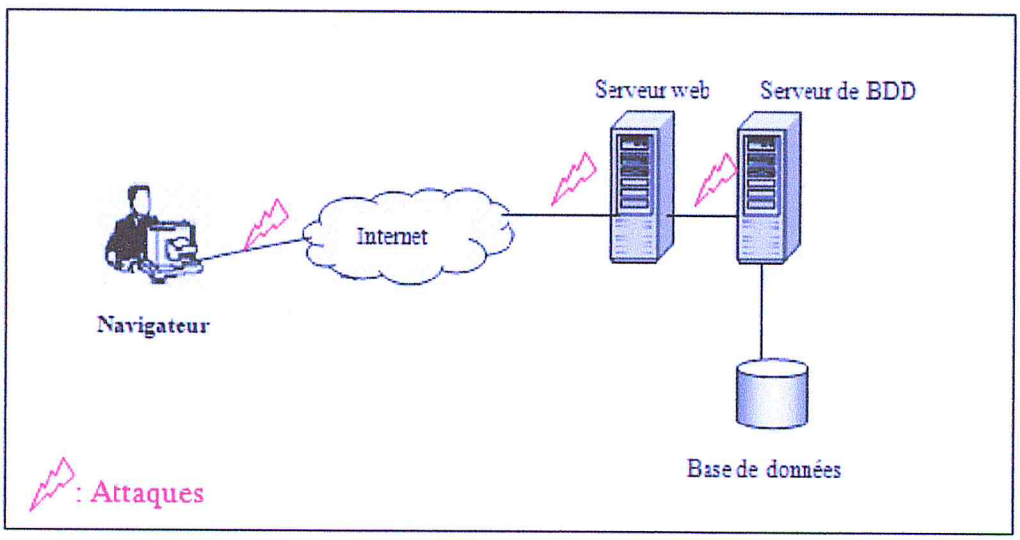


Figure 1 : Architecture d'une application web et flux menacés

2. Cryptographie

« Le chiffrement est l'action de transformation d'un texte "*lisible*" en un texte "*Illisible*", via une clé de chiffrement. Seule une personne disposant de la clé de déchiffrement (qui peut être la même que celle de chiffrement) sera en mesure de déchiffrer le texte. » **[3]**

La cryptographie est à la base de la sécurité informatique, sa connaissance est nécessaire pour comprendre les technologies de sécurité utilisées pour sécuriser les réseaux.

2.1. Définition

La cryptographie est la science d'écriture et de lecture des messages codés **[4]** . Elle permet de transmettre des données de manière confidentielle.

Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible, c'est ce qu'on appelle chiffrement ou cryptage, qui à partir d'un texte en claire donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement ou décryptage est l'action qui permet de reconstituer le texte en claire à partir du texte chiffré **[4].**

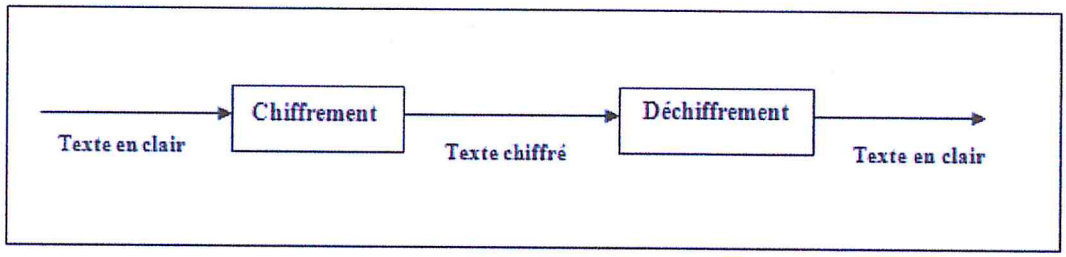


Figure 2 : Principe générale de la cryptographie.

Dans la cryptographie moderne, les transformations en questions sont des fonctions mathématiques, appelées algorithmes cryptographiques qui dépendent d'un paramètre appelé clé.

D'autres termes se réfèrent à ce domaine tel que la cryptanalyse qui est l'étude des procédés cryptographique dans le but de pouvoir décrypter des textes chiffrés et la cryptologie qui englobe les deux domaines : cryptographie et cryptanalyse **[4].**

2.2. Historique

La cryptologie a connu une évolution vertigineuse avec le développement des systèmes informatiques : passant d'une ère artisanale et confidentielle (combines et ruses déjà en 2000 av J-C) à des systèmes de très hautes technologies, nécessitant une importante puissance de calcul, essentiellement régis par l'arithmétique et des algorithmes complexes la classant ainsi parmi les sciences fondamentales. La cryptologie regroupe deux domaines : la **cryptographie** et la **cryptanalyse**.

La cryptographie du grec ***kruptos*** (caché) et ***graphein*** (écrire), qui est l'art d'écrire les messages, code des données dans le but de les rendre inexploitables par toute personne pouvant les intercepter hormis le destinataire légitime.

En parallèle au développement de la cryptographie, la cryptanalyse qui convoite à décrypter le message intercepté a progressé de façon faramineuse : les cryptanalystes s'activent au déchiffrement des systèmes les plus complexes.

Dans cette partie nous allons décrire les besoins cryptographiques, et les méthodes utiliser pour les assurée. Cette partie sera organisée comme suit :

2.3 Besoins cryptographiques

Transmettre des données de manière confidentielle, tel était le but de la cryptographie traditionnelle. Aujourd'hui la confidentialité ne suffit plus. Des services de sécurité plus élaborés sont offerts. En plus de la confidentialité, l'authentification, l'intégrité et la non répudiation sont les garanties de la cryptographie moderne **[9]** .

2.3.1. Authentification

Elle consiste simplement à vérifier l'identité de l'utilisateur ou de l'entité qui veut accéder à un système informatique.

2.3.2. Confidentialité

La confidentialité est le maintien du secret des informations… (Le petit Robert[1]).
La confidentialité peut être vue comme « la protection des données contre une divulgation non autorisée »,

2.3.3. Intégrité

permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle, elle est garantie grâce aux signatures numériques.

2.3.4. Non répudiation

Garantir la non répudiation c'est garantir qu'un correspondant ne puisse nier qu'un message lui a été envoyé. elle est assurée grâce aux signatures numériques

Pour garantir ces besoins, on utilise des méthodes basées sur des algorithmes cryptographiques que nous présenterons dans le paragraphe qui suit.

[1] ***Le Petit Robert*** est un dictionnaire de langue française, publié par les dictionnaires Le Robert.

2.4. Les méthodes de cryptographie

On distingue de type de chiffrement [3]

2.4.1. La cryptographie à clé secrète

Le chiffrement symétrique, dit aussi a clé secrète est la forme la plus ancienne de cryptage. Elle consiste utiliser une valeur courte (la clé) pour rendre un message inintelligible aux tierces parties. Elle est dite symétrique car la clé de chiffrement et celle de déchiffrement .

Principe

Le principe consiste a utiliser la même clé et le même algorithme de chiffrement pour chiffrer et déchiffrer un message. Donc les communicants doivent s'entendre a l' avance sur l'algorithme de chiffrement à employer et également sur la clé secrète à utiliser avec l'algorithme[3].

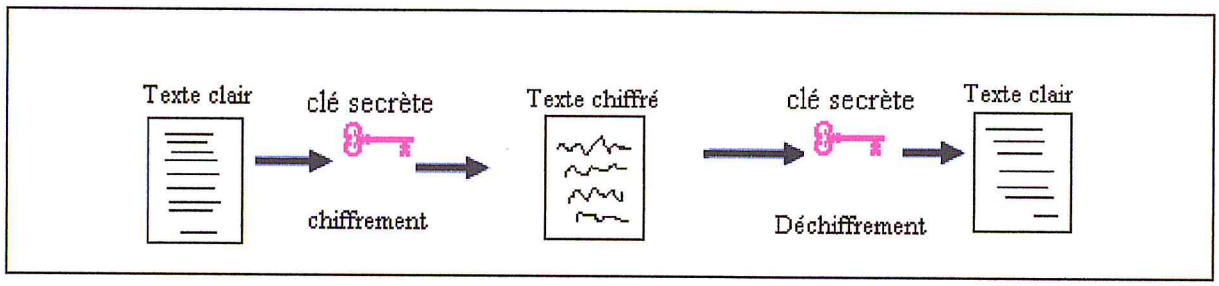


Figure 3: Chiffrement à clé secrète [7]

Il existe généralement deux types d'algorithmes symétrique, par :

a. Chiffrement symétrique par substitution :

Le code de César est le plus vieil algorithme de chiffrement symétrique par substitution connu. Il consiste à remplacer chaque lettre du message d'origine par une lettre de l 'alphabet situé n positions plus loin (par une simple translation). N constitue la clé secrète.

Exemple :

- La clé est 3 :
- Texte clair : SECURITE

- Texte chiffré: VHFXULWH

b. chiffrement symétrique par transposition :

Le principe de codage par transposition est de modifier selon une loi prédéfinie l'ordre des caractères.

La méthode de pliage constitue un exemple simple de chiffrement par transposition. Elle consiste à écrire le message d'origine dans une matrice (écriture en ligne) comportant autant de colonnes que la clé secrète. La clé secrète est constituée de numéros de colonnes. Le cryptogramme est obtenu en lisant cette matrice en colonnes selon l'ordre défini par la clé.

Exemple :

Le message d'origine: COMMERCE ELECTRONIQUE
La clé de codage : 4312
Le message crypté : MECNE MCEOU CEETI ORLRQ

1	2	3	4
C	O	M	M
E	R	C	E
E	L	E	C
T	R	O	N
I	Q	U	E

2.4.1.3. Les avantages et inconvenants de la cryptographie à clé secrète

Le chiffrement symétrique est intéressant car il est simple à mettre en œuvre et requiert un faible temps de calcul. Mais il présente un inconvénient majeur : la difficulté de protéger le secret d'une clé. En effet, au moment ou les deux parties échangent leur clé secrète, ils ne peuvent pas s'assurer que celle ci n'est pas interceptée par un tiers. Cette solution s'avère donc, seule, insuffisante.

Ce problème a incité à la réflexion à une autre méthode cryptographique plus sûre et moins complexe en matière de gestion. La cryptographie à clé publique est apparue.

2.4.2 .La cryptographie à clé publique

Le chiffrement asymétrique, dit aussi a clé publique découle de découvertes théoriques relativement récentes dans le domaine mathématique. Il repose sur l'existence de fonctions mathématiques difficiles à inverser **[7].**

Principe

Chaque communicant utilisent deux clés, l'une est connue par tous (clé publique), l'autre n'est connue que par lui-même (clé privée). Le message crypté avec l'une ne peut être décrypté qu'avec l'autre

Les deux clés sont reliées mathématiquement entre elles de telle sorte qu'il est impossible de retrouver la clé privée en connaissant la clé publique.

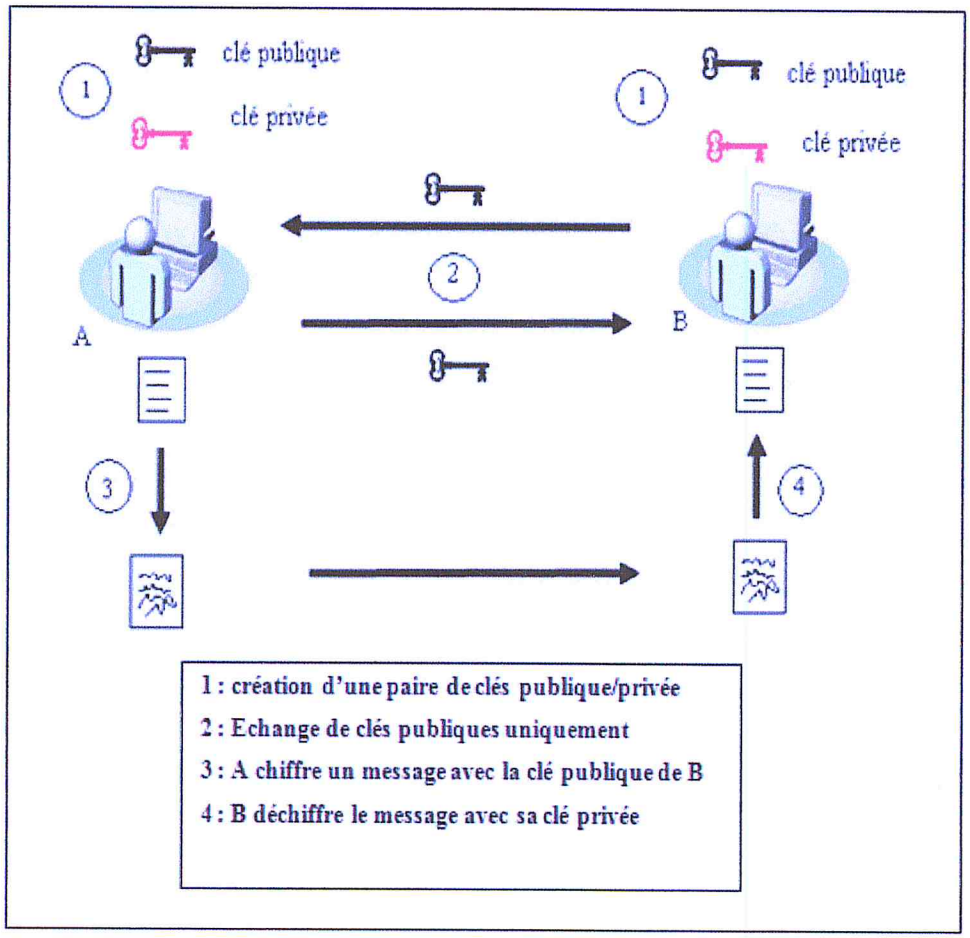


Figure 4 : Chiffrement à clé publique**[3]**

Parmi les algorithme de cryptage asymétrique il y a l'algorithme DSA et RSA, nous allons utiliser le RSA , vue qu'il est très utiliser en public, simple et fiable , nous allons expliquer le principe ainsi les points fort et faible du RSA.

*2.4.2 .1.*L'algorithme RSA : *(Rivest Shamir Adleman)*

Inventé à la fin des années 1970 (de ses concepteurs Rivest, Shamir et Adleman), il utilise des clés très longues (jusqu'à 1024 bits) et offre toutes les garanties cryptographiques (confidentialité, intégrité, authentification et non répudiation). La sécurité apportée par le système RSA se fonde sur la difficulté à factoriser le produit de deux grands nombres premiers. Le RSA reste sécurisé face aux attaques, mais on doit employer des nombres premiers de plus en plus grands, car la puissance des microprocesseurs croît sans cesse . Cet algorithme est très largement utilisé, par exemple dans les navigateurs pour les sites sécurisés et pour chiffrer les emails. Il est dans le domaine public.

Le principe

Pour encrypter un message, on fait: $\mathbf{c = m^e \bmod n}$

Pour décrypter: $\mathbf{m = c^d \bmod n}$

m = message en clair
c = message encrypté
(e,n) constitue la clé publique
(d,n) constitue la clé privée
n est le produit de 2 nombres premiers
mod est l'opération de modulo (reste de la division entière)

Créer une paire de clés

Pour créer une paire de clés, il ne faut pas choisir n'importe comment **e**, **d** et **n**. Voici comment procéder:

1. Prendre deux nombres premiers **p** et **q** (de taille à peu près égale). Calculer **n = pq**.
2. Prendre un nombre **e** qui n'a aucun facteur en commun avec **(p-1)(q-1)**.
3. Calculer **d** tel que **e*d mod (p-1)(q-1) = 1**

Le couple **(e, n)** constitue la clé publique. **(d, n)** est la clé privée.

Pour crypter on fait : $c = m^e \bmod n$

Pour décrypter on fait : $m = c^d \bmod n$

2.4.2 .2.Problème de la cryptographie à clé publique

Les méthodes de chiffrement à clé publique sont jusqu'à 1000 fois plus lentes que les méthodes de chiffrements à la clé secrète.

2.4.2.3. Cryptographie symétrique *vs* cryptographie asymétrique

- **vitesse de chiffrement :**

La vitesse de chiffrement est le plus grande point qui creuse l'écart entre les deux méthodes de chiffrement, par exemple nous savons que le standard DES est 1000 fois plus rapide que le RSA.

- **Distribution des clés :**

La distribution des clés secrètes est un problème, car l'expéditeur et tous ses destinataires partagent la même clé, ce qui devient pratiquement impossible à contrôler sous un réseau de grande envergure tel qu'Internet. Dans les petits réseaux, le changement régulier de la clé secrète est indispensable. Contrairement aux clés secrètes, dans le cas asymétrique les clés de chiffrement sont rendues publiques et ceci sans compromettre la sécurité du message crypté car les clés de déchiffrement sont privées.

Voici un tableau qui résume les avantages et inconvénients des deux systèmes de chiffrement

Type de crypto système	Avantages	Inconvénients
Clé symétrique	• Rapide • Peut être facilement réalisée sur une puce	• Difficulté de distribuer les clés • Ne permet pas de signature électronique
Clé publique	• Utilise deux clés différentes • Fournit des garanties d'intégrité et de non répudiation par signature électronique	• Lent et demandant beaucoup de calculs

Tableau II.1 Avantages et inconvénients des deux systèmes cryptographiques

2.4.3. Hachage

Principe

Le hachage (appelé aussi résumé de message ou empreinte numérique) est une représentation plus bref d'un message.

La fonction de hachage reçoit en entrée un message de longueur aléatoire et produit un message de longueur fixe .

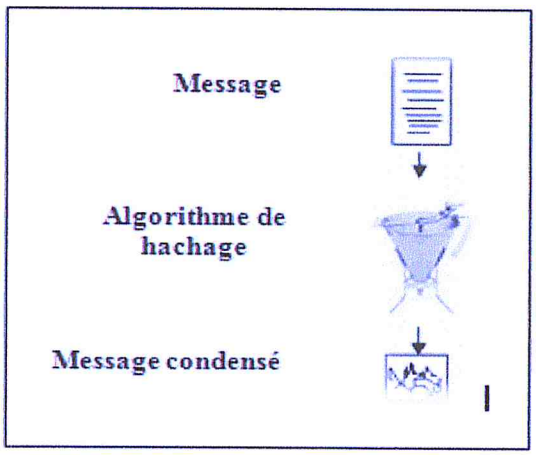


Figure 5 : Principe du hachage.

Un algorithme de hachage doit être :

- Cohérent : le même message en entrée doit toujours produire le même résultat.
- Unique : deux messages différents ne doivent jamais produire le même condensé.
- Non réversible : il doit être extrêmement difficile, voir impossible d'obtenir le message d'origine à partir de son condensé.

Le hachage est généralement utilisé pour fournir une empreinte d'un message ou fichier pour assurer l'intégrité et l'authentification du message.

2.4.3.1. Types de hachage

Les algorithmes de hachage peuvent être sans clé ou avec, on distingue trois types de hachage :

- **Hachage sans clé : MIC** (Message Integrity Code)

Dans ce type, le message est soumis à un algorithme de hachage sans clé (sans paramètre en entrée). Les algorithmes les plus utilisés sont MD5 et SHA1.

La plupart des signatures numériques à clé publique emploient des résumés de message sans clé.

- **Hachage avec clé : MAC** (Message Authentification Code)

Dans ce type, le message est soumis à une fonction de hachage qui reçoit comme paramètre d'entrée une clé.

- **HMAC :**(keyed-Hash Message Authentication Code)

Combine les deux méthodes précédentes. Le message est concaténé à une clé secrète. Le tout est soumis à une fonction de hachage sans clé.

2.4.4. Signature numérique :

2.4.4.1. Définition :

Une signature numérique est un **condensé de message crypté** qui joint un document. Elle combine l'utilisation du cryptage à clé publique et d'une fonction de hachage.

Ce ci permet de s'assurer que :
- l'expéditeur est bien l'émetteur de message (identification - authentification)
- le message reçu est bien conforme à celui transmis par l'expéditeur (intégrité)

.4.4.2. Processus de création d'une signature :

- Créer une paire de clés publique/ privée
- Soumettre le message à une fonction de hachage
- Crypter le résultat de hachage avec la clé privée

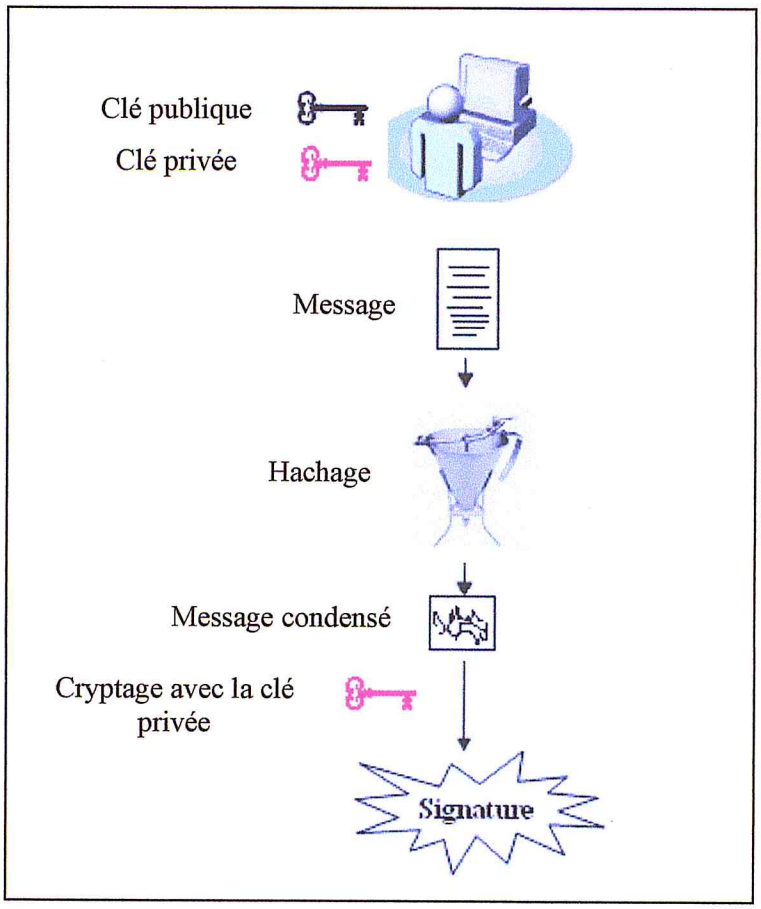


Figure 6: processus de création d'une signature

Remarque :

L'émetteur envoie au destinataire son message en lui concaténant la signature obtenue et la clé publique (ou un certificat numérique contenant la clé publique). La clé publique servira pour la vérification de la signature.

2.4.4.3. Processus de vérification d'une signature :

Le destinataire reçoit un message signé avec la clé privée. La clé publique correspondante à cette dernière est à sa disposition. Pour vérifier cette signature et donc vérifier que le message provient du bon émetteur, il procède ainsi :

1. Séparer la signature du message
2. Décrypter la signature avec la clé publique de l'émetteur (on obtient ainsi le résumé du message originale).

3. Soumettre le message à la même fonction de hachage (les communiquant s'entendent sur l'algorithme de hachage avant de commencer l'échange de message)
4. Comparer le résumé obtenu dans 3 avec celui obtenu dans 2.

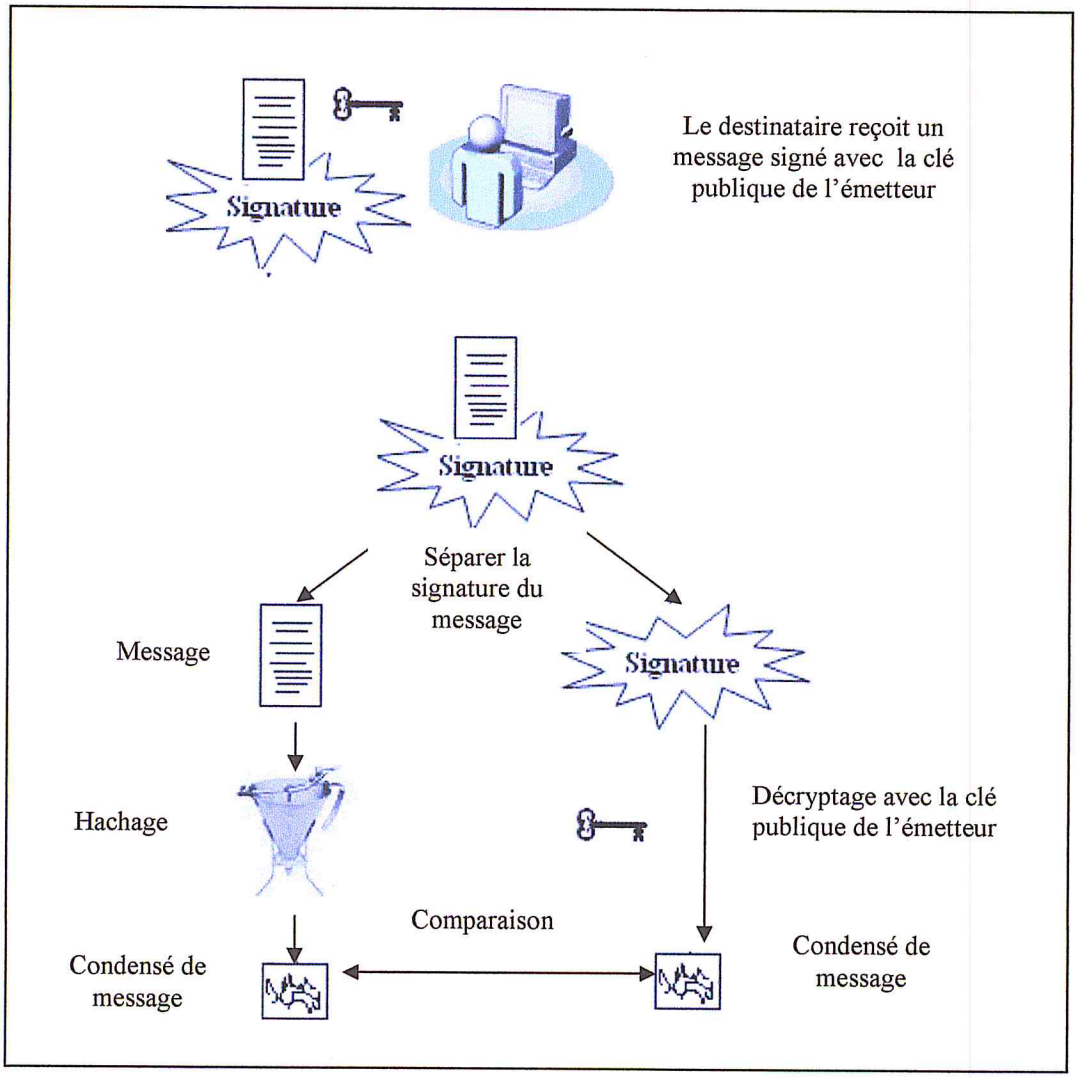


Figure 7: Vérification d'une signature

3. Quelques protocoles de sécurité :

a- Dans la couche réseau

La section suivante décrit le protocole IPSec qui est utilisé pour la sécurité dans la couche réseau.

***IP Sec :* (IP Security) :**

C'est un protocole destiné à fournir différents services (critères) de sécurité. Il propose ainsi plusieurs choix et options qui lui permettent de répondre de façon adaptée aux besoins des entreprises. Néanmoins, son intérêt principal reste sans conteste son mode dit de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres choses de créer des réseaux privés virtuels.

IPsec est facultatif sur IPv4 mais est obligatoire sur IPv6. IPsec a d'autres avantages que la sécurisation du trafic, il permet par exemple d'économiser la bande passante grâce à la compression des en-têtes des paquets. IPsec est composé de plusieurs protocoles différents : AH, ESP, IPcomp et IKE [8].

Le protocole AH : Le protocole AH (Authentification Header) permet de garantir l'authenticité des paquets échangés en leur inscrivant une somme de contrôle (de l'en-tête IP jusqu'à la fin du paquet) chiffrée.

Le protocole ESP : Le protocole ESP (Encapsulating Security Payload) encrypte toutes les données du paquet garantissant leur confidentialité.

Le protocole IPcomp : Le protocole IPcomp (IP payload compression) permet de compresser un paquet avant de le chiffrer avec ESP.

Le protocole IKE : Le protocole IKE (Internet Key Exchange) est utilisé pour l'échange des clés utilisées pour l'encryptage.

b- Dans la couche transport

Il existe plusieurs protocole de sécurité de transport de données tel que SSL, SSH…, ils sont classés dans cette catégorie de protocole de sécurité car leur objectif est de sécurisé la couche transport et de fournir également des méthodes qui assurent la confidentialité, l'authentification et l'intégrité au dessus de celle-ci. La section suivante décrit un de ces protocoles le « SSL ».

4.Le protocole SSL (Secure Socket Layer)

4.1. Historique

SSL a été développé par Netscape en 1994. la version 2 a été lancée en 1995.Un produit concurrent de Microsoft (PCT Private community Technology) apparu en 1995 a poussé Netscape à lancer la version3 de SSL dans la même année.
En 1996, l'IETF (Internet Engeneering Task Force) constitua un comité pour développer et publier un **standard** SSL.

En Janvier 1999, on a publié TLS (Transport Layer Security), fondé sur SSL version 3. Il est géré par Microsoft et Netscape.

4.2.Définition :

« SSL (Secure Sockets Layers, que l'on pourrait traduire par couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet. Le standard SSL a été mis au point par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet. Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.
Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP. En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, située entre la couche application et la couche transport (protocole TCP par exemple).
De cette manière, SSL est transparent pour l'utilisateur (entendez par là qu'il peut ignorer qu'il utilise SSL). Par exemple un utilisateur utilisant un navigateur internet pour se connecter à un site de commerce électronique sécurisé par SSL enverra des données chiffrées sans aucune manipulation nécessaire de sa part. » **[20].**

4.3.Les fonctionnalité de SSL

SSL et TLS proposent les fonctionnalités suivantes[9] :

Authentification :Le client doit pouvoir s'assurer de l'identité du serveur. Depuis SSL 3.0, le serveur peut aussi demander au client de s'authentifier. Cette fonctionnalité est assurée par l'emploi de certificats.

Confidentialité : Le client et le serveur doivent avoir l'assurance que leur conversationne pourra pas être écoutée par un tiers. Cette fonctionnalité est assurée par un algorithme de chiffrement.

Identification et intégrité : Le client et le serveur doivent pouvoir s'assurer que les messages transmis ne sont ni tronqués ni modifiés (intégrité), qu'ils proviennent bien de l'expéditeur attendu. Ces fonctionnalités sont assurées par la signature des données.

4.4. Applications de SSL [10]

Le protocole SSL permet la sécurisation de tout protocole applicatif qui s'appuie sur la pile TCP/IP, tels que HTTP, LDAP, SMTP, FTP, etc. Nous explicitons dans la suite quelques exemples :

- **HTTPS**

Le HTTP (HyperText Transfert Protocol) est le protocole le plus utilisé sur Internet. C'est un protocole client/serveur utilisé pour transférer les documents entre le serveur HTTP et le navigateur web lors de la consultation d'un site web.

HTTP protège peu la confidentialité des données. En effet les documents sont transmis sans être chiffrés.

Pour améliorer la confidentialité, on utilise le protocole HTTPS (HTTP over SSL).

La sécurité offerte par HTTPS réside dans le fait qu'il authentifie le client et le serveur grâce au certificat numérique. Il chiffre également la communication (garanties apportées par SSL)

Il est généralement utilisé pour les transactions financières en ligne: commerce électronique, banque en ligne. Il est même utilisé lors d'une simple inscription à un site web pour des raisons de confidentialité.

- **LDAPS**

LDAP (Lightweight Directory Access Protocol) est un protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP. Un annuaire LDAP respecte généralement le modèle X.500 (X.500 désigne l'ensemble des normes informatiques sur les services d'annuaire).

Pour sécuriser les communications LDAP, l'implémentation de SSL constitue la meilleure solution. A ce moment, on parle de LDAPS (LDAP over SSL).

- **SMTPS**

Le protocole SMTP (Simple Mail Transfer Protocol, traduisez Protocole Simple de Transfert de Courrier) est le protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point. Le courrier est remis directement au serveur de courrier du destinataire. SMTPS est le protocole SMTP au dessus de la couche SSL.

- **IMAPS**

Le protocole IMAP (Internet Message Access Protocol) permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur IMAP). Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion. IMAPS est le protocole IMAP au dessus de la couche SSL.

4.4.1.Mise en œuvre d'un service HTTPS

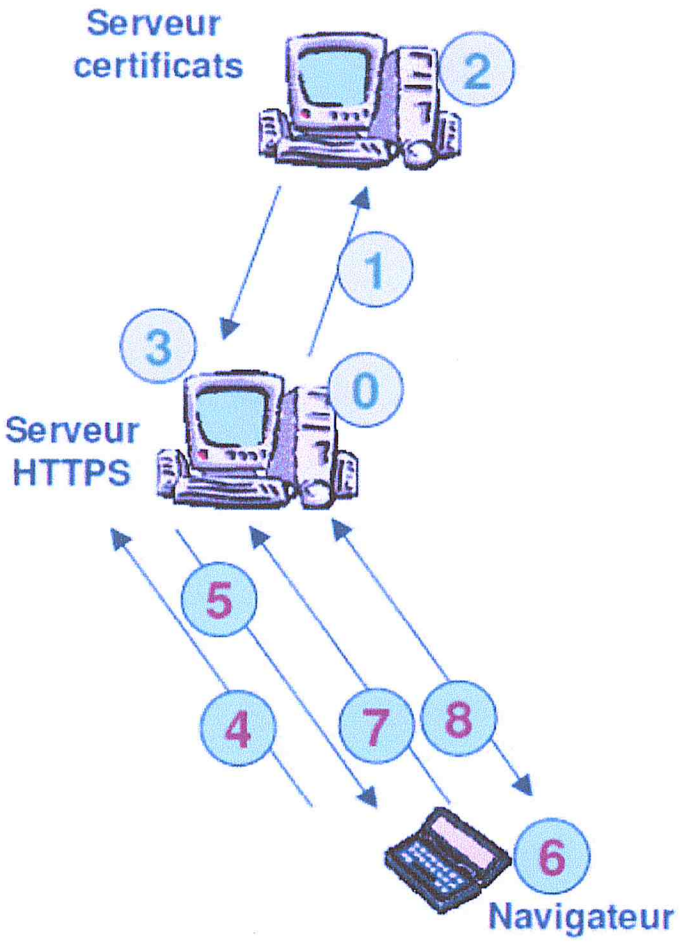


Figure 8. Etapes de la mise en œuvre d'un service HTTPS **[20].**

Phase « Mise en production »

0 : Génération clé publique / clé privé.

1 : Demande auprès d'une autorité (publique) d'un certificat serveur.

2 : Génération du certificat serveur.

3 : Installation du certificat serveur sur le Serveur Web.

Phase « Navigation internaute »

4 : Ouverture connexion SSL : « clic sur URL https://www.x.dz ».

5 : Envoi certificat du serveur vers le client.

6 : Génération clé de session symétrique.

7 : Envoi clé symétrique (chiffrée avec clé publique du serveur).

8 : Echanges protégés (confidentialité, intégrité).

4.5.Les points fort et faible du SSL

Les points fort :

- L'indépendance vis à vis des couches inférieures et supérieures
- Le fonctionnement en mode Client/serveur
- L'assurance aux deux parties d'une transaction authentifiée (certificats), privée (cryptage) identifiée et intègre (MAC).

Les points faible

- SSL/TLS ne protège pas contre l'analyse du trafic, c'est à dire contre les cryptanalystes qui s'intéresse aux adresses sources et destinations.
  En effet SSL/TLS est situé au dessus de la couche transport dans la pile des protocoles. Il n'a donc aucun moyen de masquer l'adresse et le port des adresses sources et de destinations.
- La négociation des paramètres cryptographiques se fait en claire sans chiffrement.

5. Conclusion

Les méthodes et outils pour la sécurité web deviennent de plus en plus nécessaire pour faire face aux logiciels espion.

Nous avons abordé dans ce chapitre les différentes méthodes cryptographiques, notamment la cryptographie à clé publique sur laquelle se base le protocole SSL, protocole de sécurisations des transactions entre un client et un serveur. SSL a donné naissance au protocole HTTPS, et bien d'autres que nous avons décrit brièvement.

PARTIE 2

CONCEPTION ET REALISATION

CHAPITRE 3

CONCEPTION

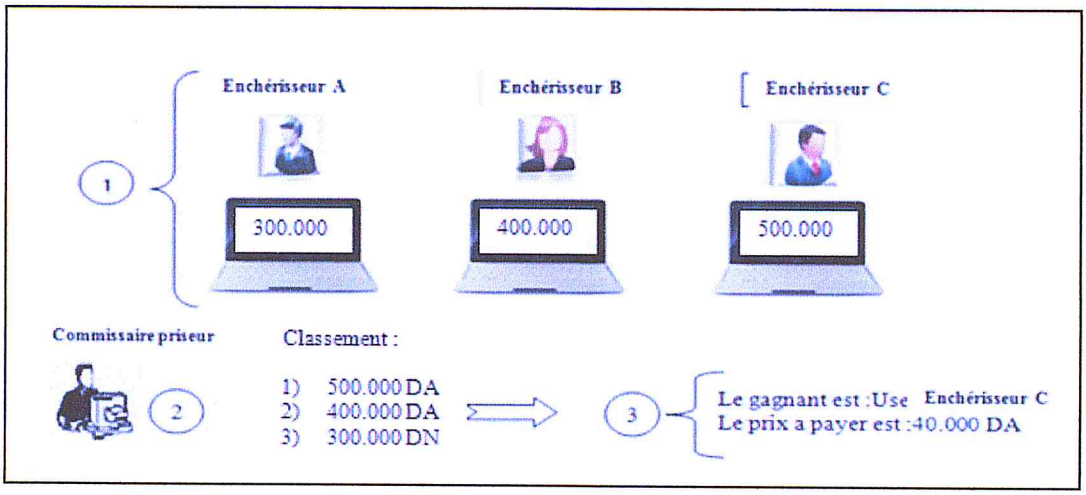


Figure 9 : le processus ordinaire du protocole d'enchère vickery

1- Chaque participant soumet une offre une seul fois et en un seul tour ,sans connaitre les offres des autre participants.
2- Le commissaire priseur classent les prix soumise en ordre croissant .
3- Le commissaire priseur choisi le participant qui soumis la plus grande offre et lui faire payer le 2eme prix classé .
4-

2.1.1. Le problème d'enchère vickery:

Le problème qui se pose en utilisant ce protocole d'enchère est que l'initiateur de l'enchère « l'administrateur du site » peut falsifier la seconde offre, sans que les participants ne se rendent compte. Ainsi Celui qui remportera l'enchère risque de payer plus qu'il n'en faut. Le problème est illustré dans le schéma suivant :

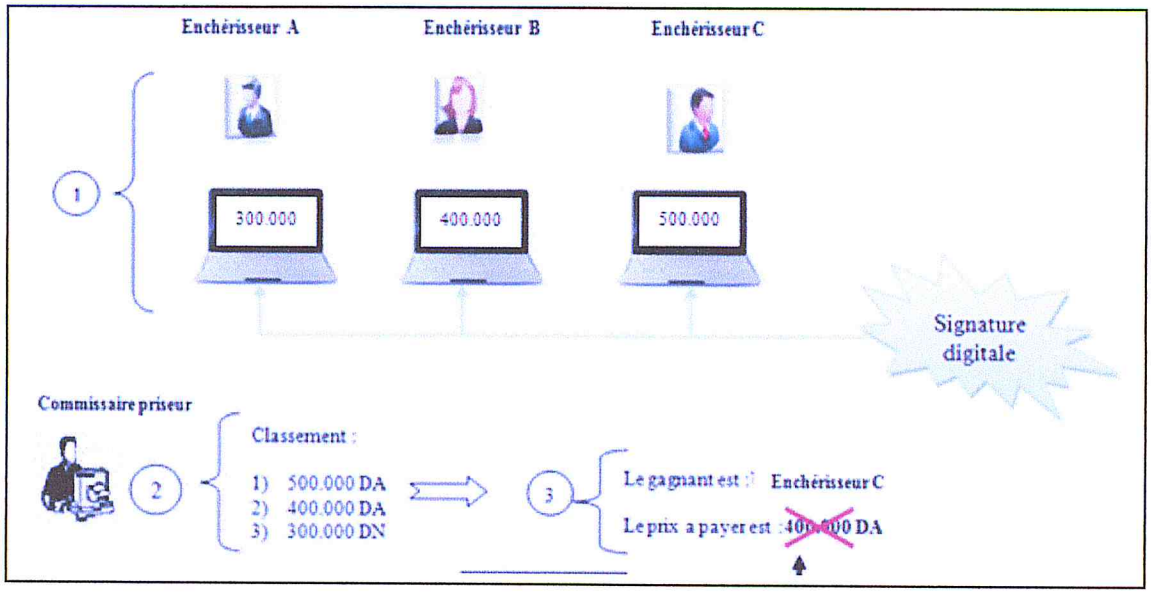


Figure 10 : un schéma illustrant le problème de l'enchère vickrey

2.1.2.La solution proposer pour l'enchère vickery:

Afin de pallier a ce problème nous allons utiliser la signature digitale « électronique-numérique » qui permet de garantir L'intégrité des prix soumis par les enchérisseurs, nous allons expliquer en utilisant un exemple le mécanisme de la signature digitale .

1- Générer la paire de clé (public, privé) ,en utilisant l'algorithme RSA :

La clé privé sert a signer, la clé public sert a vérifier la signature .

Génération des clés (public ,privé) suivant l'algorithme RSA est la suivante :

- On prend 2 nombres premiers au hasard: **p** = 29, **q** = 37
- On calcul **n** = p*q = 29 * 37 = 1073
- On choisir **e** au hasard tel que **e** n'a aucun facteur en commun avec (p-1)(q-1):
- (p-1)(q-1) = (29-1)(37-1) = 1008
- On prend **e** = 71
- On choisit **d** tel que 71*d mod 1008 = 1
- On trouve **d** = 1079

On a maintenant nos clés :

- La clé publique est (e ,n) = (71,1073)
- La clé privée est (d, n) = (1079,1073)

2- **Soumettre le prix a une fonction de hachage suivant l'algorithme SHA1 on obtient :**

Prix haché= 58116da64ae33beb98e9

3- **Crypter le hache obtenu avec la clé privé** (1079,1073)

Tout d'abord on traduit le hache en code ASCII puis on le découpe en blocs qui comportent moins de chiffres que **n=**(1073), **n** comporte 4 chiffres, donc on va découper notre message en blocs de 3 chiffres.

C = 581 161 006 564 651 013 398 101 989 810 190

On crypte chaque blocs avec la clé privé suivant l'algorithme RSA :

$Signature_i = c_i^{\,e} \bmod n$ / i=nombre de blocs obtenus.

$Signature_1 = 581^{1079} \bmod 1073 = 639$

et ainsi de suite jusqu'à obtenir la signature digitale complète du prix mentionné.

Avec cette méthode même l'administrateur du site ne pourra pas connaître les offres soumises.

La vérification de la signature :

Consiste a décrypter la signature avec la clé public (e,n) =(71,1073) correspondante à la clé privée de cryptage en utilisant l'algorithme RSA pour avoir le hache ,puis le décompresser en utilisant le même algorithme de hachage SHA1 :

Hache = signature ^{e} mod n

Le prix originale est obtenu on décompressant le hache obtenu .

2.2.Le deuxième axe :

Nous rappelons qu'une plateforme e-commerce est une application web dont l'architecture globale est la suivante :

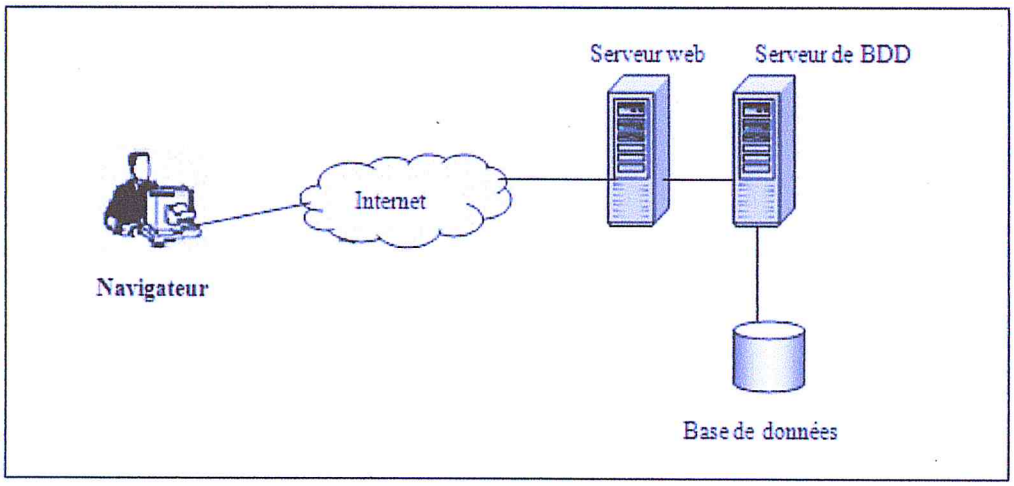


Figure 11: Architecture d'une application web

2.2.1.Besoins en sécurité

Une plateforme e-commerce est une application web dont les flux de données menacés sont présentés dans la figure suivante :

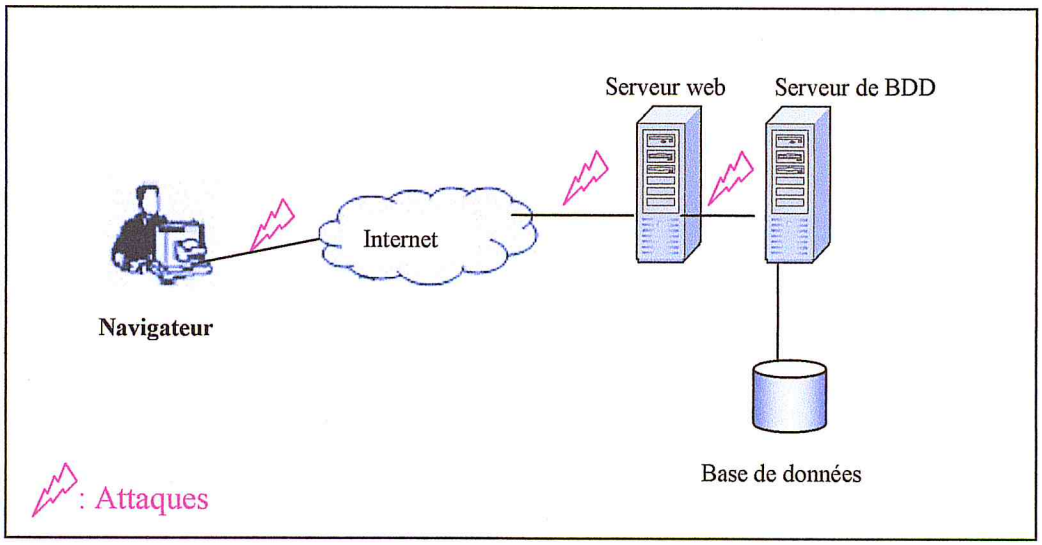


Figure 12: Architecture d'une application web et flux menacés

Dans l'interaction entre le client et le serveur web, un navigateur web transmet des données au serveur web. Elles sont transférées à l'application qui entre en interaction avec la base de données. En suivant ces routes, nous pouvons repérer les points faibles dans la communication entre le client et le serveur web, et la communication entre le serveur web et le serveur de base de données. **[19]**

- **Communication entre utilisateur et serveur web**

La communication d'un client avec le serveur via Internet se fait avec le protocole HTTP . Cependant, le trafic HTTP n'est pas sécurisé. Un pirate peut facilement intercepter les données transférées entre le client et le serveur, injecter de fausses informations, usurper l'identité d'un client ou un serveur, etc. autrement dit , on n'est pas sûr d'être avec le bon serveur ou le bon client. Dans les plateforme e-commerce ceci présente un risque dans des cas tels que :

- Interception d'informations personnelles .
- Interception d'une communication confidentielle .
- Injection de fausses informations .
- Usurpation de l'identité d'un client, d'un d'administrateur. Une anarchie totale en résulte.

- **Communication entre serveur web et serveur de base de données**

Le serveur web et le serveur de base de données s'exécutent probablement sur des machines différentes et la base de données d'une plateforme e-commerce peut contenir des données confidentielles (mot de passe, données confidentielles, etc.), il faut donc trouver un moyen pour sécuriser les communication entre les deux serveurs. **[19]**

En résumé, pour obtenir une plateforme e-commerce sécurisée, on doit garantir :

- La sécurisation de la communication entre le client et le serveur (authentification du client/serveur, chiffrement du trafic entre eux) .
- La sécurisation des objets de la base de données (chiffrement des données confidentielles) .
- La sécurisation des outils de communication et de collaboration offerts par la plateforme tels que la messagerie.

2.2.2.La solution proposer:

Pour pallier a ce problème nous allons utiliser le protocole HTTPS (HTTP over SSL).

La sécurité offerte par HTTPS réside dans le fait qu'il authentifie le client et le serveur grâce au certificat numérique. Il chiffre également la communication (garanties apportées par SSL).

Le schéma suivant résume l'enchaînement des besoins qui délimitent le travail à réaliser :

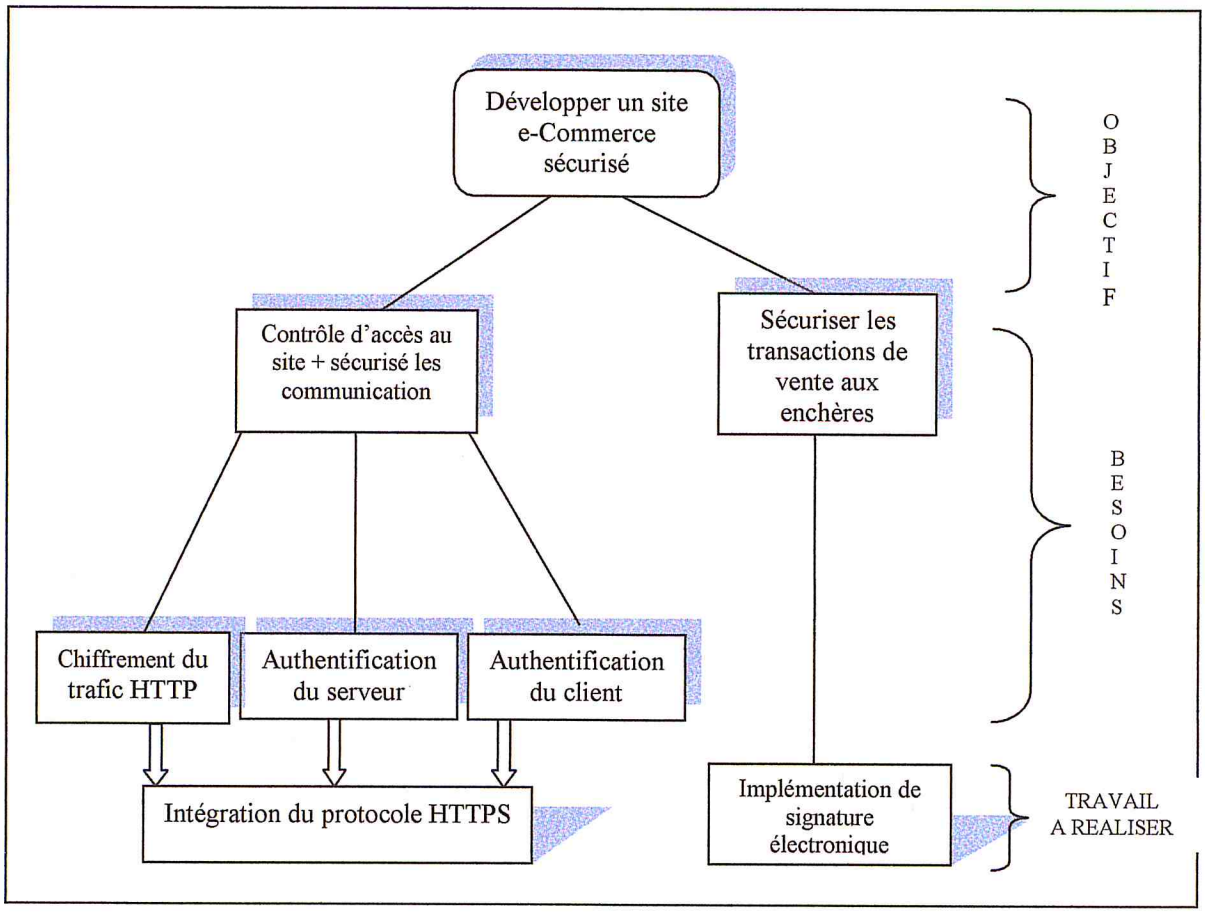


Figure 13 : Organigramme délimitant le contexte de notre travail

Les parties à développer dans ce travail sont:

- Développer un site web e-Commerce
- Automatiser le protocole d'enchère vickery
- Sécurisé les transactions de vente aux enchères «vickery ».
- Securisé la communication sur notre site
-

3. Architecture fonctionnelle du système :

L'administrateur s'occupe des tâches suivantes:

- **La gestion des clients :** elle comprend la suppression et la recherche d'un client et l'affichage de la liste clients.

- **La gestion des produit :** elle comprend la modification, la suppression et la recherche d'un produit, affichages des produits .
- **La gestion des demande :** elle comprend la modification, la suppression et la d'une demande, affichages des demandes en ligne.

- les principales tâches du client sont:
  - **Inscription**
  - **Déposer un produit:** elle consiste a mettre un produit aux enchères .
  - **Enchérir un produit** consiste a enchérir le produit met aux enchères suivant le protocole d'enchère vickery.
  - **Rédiger une demande d'un produit.**

- Les taches suivants sont faites automatiquement par notre système
  - Automatiser l'enchère vickrey
  - Sécuriser la transaction de vente aux enchère
  - Sécuriser la communication dans notre système

4. Modélisation de notre système

Pour modéliser les différents processus de notre système nous avons choisi d'utiliser UML (Unified Modeling language),qui est un langage de modélisation graphique et textuel destiné à décrire des besoins, spécifier, documenter des systèmes et architectures logicielles et concevoir des solutions **[14].**

Dans cette section nous allons représenter les diagrammes de cas d'utilisation et les diagrammes de séquence, dans le but de spécifier les différentes fonctionnalités offertes par notre système .

- Les diagrammes de cas d'utilisation : qui servent à donner une vision globale de notre système.
- les diagrammes de séquence qui montrent les différentes fonctionnalités offertes par le système d'une manière chronologique.
- les diagramme d'activité pour montrer l'enchaînement des actions et décisions au sein d'une activité .

4.1.Diagrammes de cas d'utilisation

La représentation par diagramme de cas d'utilisation permet de voir de façon simple les différents acteurs, comment est délimité le système, les fonctionnalités demandées au système, et les rôles des différents acteurs vis-à-vis du système. **[13]**

Suit à l'analyse de notre système d'enchère nous avons dégagé les diagrammes de cas d'utilisation suivants :

- Diagramme de cas d'utilisation inscription
- Diagramme de cas d'utilisation consulter le site
- Diagramme de cas d'utilisation consulter le panel personnel
- diagramme de cas d'utilisation enchérir un produit.
- diagramme de cas d'utilisation globale du vendeur.
- diagramme de cas d'utilisation globale d'administrateur

4.1.1. Diagramme de cas d'utilisation « inscription »

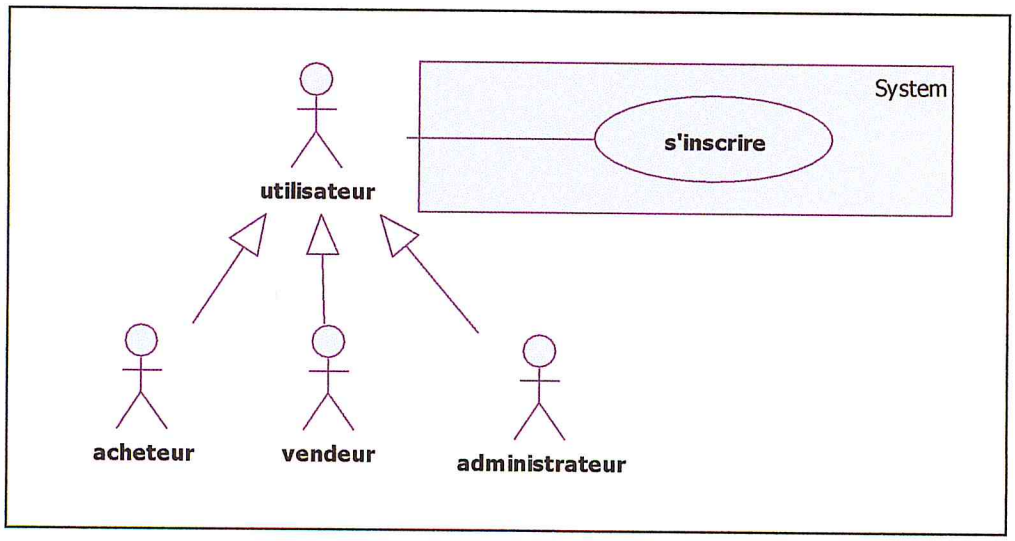


Figure 14: Diagramme de cas d'utilisation « inscription »

Scénario d'inscription:

Résumé :ce cas d'utilisation permet a l'utilisateur d'avoir un compte sur notre site afin de pouvoir réaliser les fonctionnalité offerte par notre système .

Scénario nominal :

1- l'utilisateur accède a l'interface d'inscription .
2- il remplie le formulaire d'inscription
3- le système vérifie les informations saisie .

4- si les informations sont valides le système affiche une page de confirmation d'inscpription,sinon un message d'erreur.

4.1.2. Diagramme de cas d'utilisation « consulter le site »

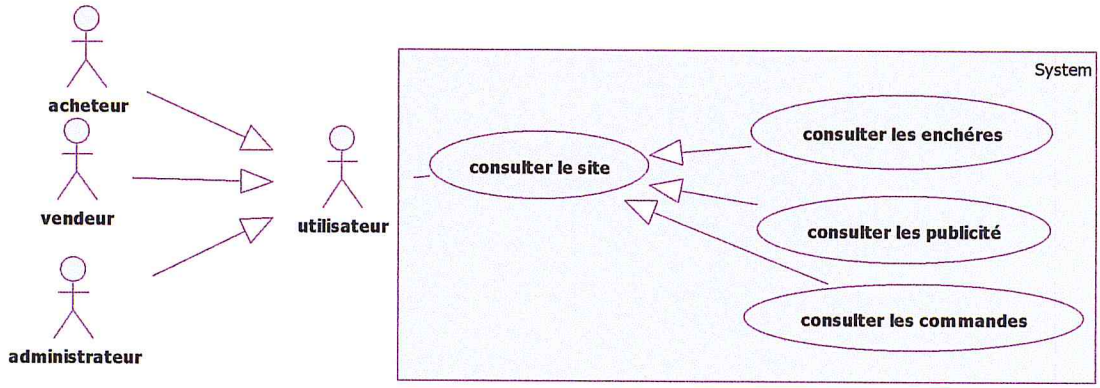


Figure 15: Diagramme de cas d'utilisation « consulter le site »

Ce cas d'utilisation permet aux utilisateurs de voir les produits mise aux enchères , les publicité ,les demandes mises.

4.1.3. Diagramme de cas d'utilisation « consulter le panel personnel »

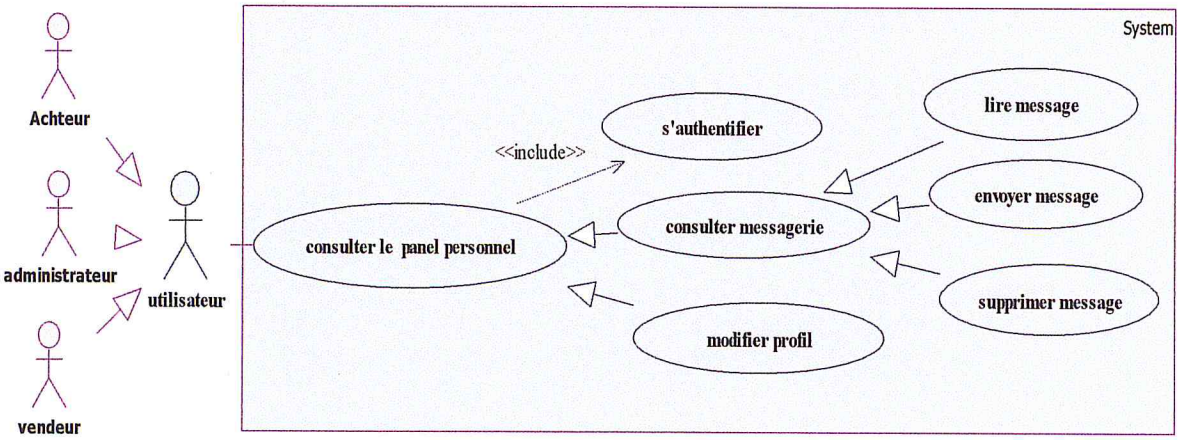


Figure 16: Diagramme de cas d'utilisation « consulter le panel personnel »

Scénario consulter panel personnel:

Résumé :ce cas d'utilisation permet a l'utilisateur d'accéder a son compte personnel.

Scénario nominal :

1- l'utilisateur s'authentifie .

2- le système vérife l'identité de l'utilisateur .

3- si l'utilisateur existe ,le système ouvre une session sécurisé « https »

Scénario consulter modifier profil:

Résumé :ce cas d'utilisation permet a l'utilisateur de modifier son profil.

Scénario nominal :

1- l'utilisateur s'authentifie .
2- il accède a la page de modification
3- l'utilisateur saisie les modifications .
4- le système vérifie les modifications saisie et la confirme

Scénario consulter messagerie :

Résumé :ce cas d'utilisation permet a l'utilisateur de contacter l'administrateur du site seulement ,il peut envoyer des messages, recevoir des messages de l'administrateur, et consulter les messages envoyés.

4.1.4. diagramme de cas d'utilisation enchérir un produit

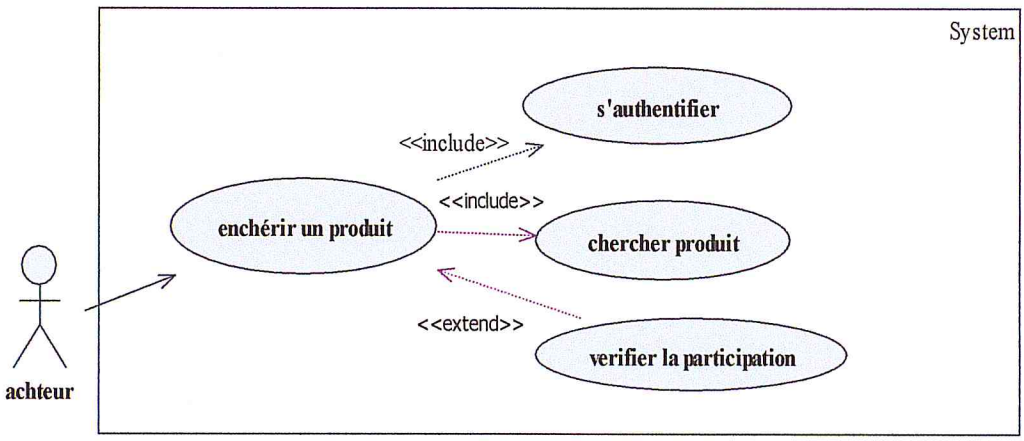


Figure 17: Diagramme de cas d'utilisation enchérir un produit

Description du Scenario enchérir un produit :

Résumé :

Ce cas d'utilisation permet aux acheteurs d'enchérir un produits mise aux enchères :

Pré-condition :

- Utilisateur authentifié.

- L'utilisateur possède les droits d'accès.

Scénario nominal :

1. L'acheteur s'authentifie
2. Il cherche le produit a enchérir.
3. Le système affiche le produit avec son détail ainsi il donne accès a la participation seulement si l'utilisateur n'a pas encore participer en affichant une zone de saisie pour le prix.
4. Sinon il affiche un message de duplication.

4.1.5. diagramme de cas d'utilisation globale d'un Vendeur

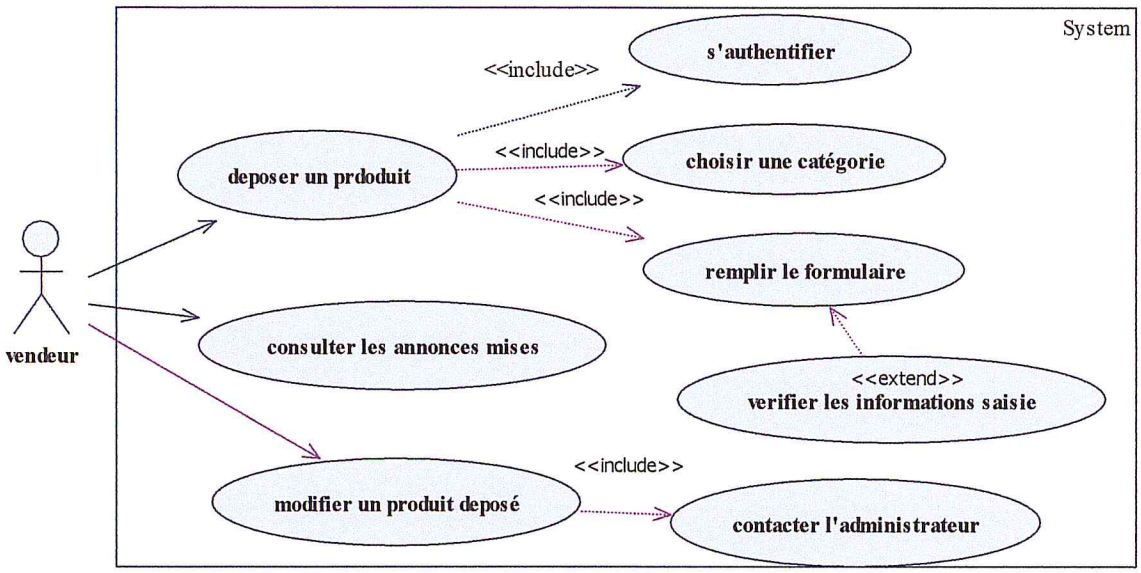


Figure 18:Diagramme de cas d'utilisation globale d'un vendeur

Description du Scenario déposer un produit:

Résumé :

Ce cas d'utilisation permet au vendeur de mettre son produit aux enchères :

Scénario nominal :

1. Le vendeur s'authentifier.
2. Le vendeur choisie la catégorie du produit a déposer.
3. Le système affiche le formulaire adéquat a cette catégorie .
4. Le vendeur remplie le formulaire
5. Le système vérifie les informations saisie

6. Le système affecte une date début /fin d'enchère pour ce produit(la date début est la date de dépôt ,la date de fin est fixer a 7jours)

4.1.6. diagramme de cas d'utilisation globale d'administrateur

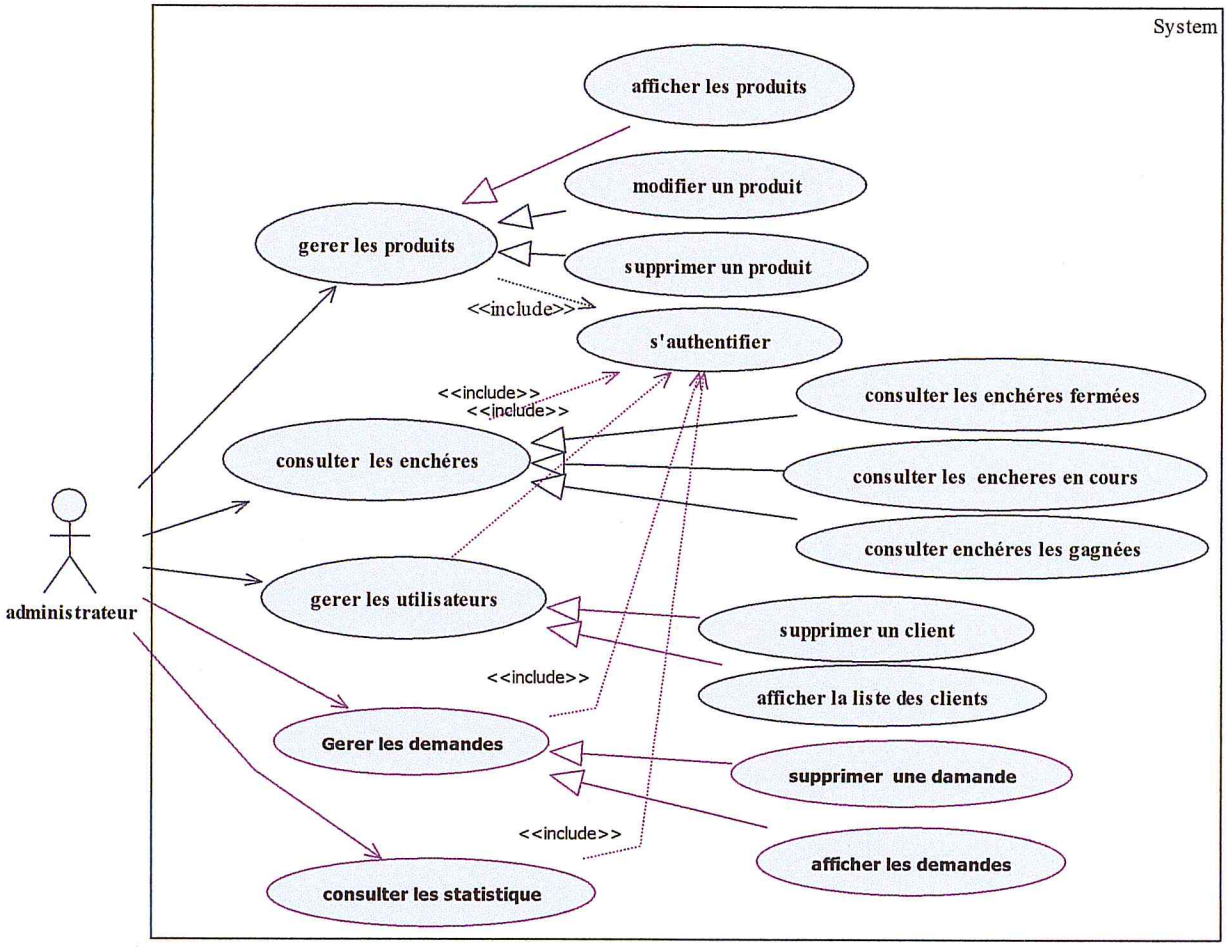


Figure 19:Diagramme de cas d'utilisation globale de l'administrateur

Description du Scenario:

Résumé :

Ce cas d'utilisation est général , il permet a l'administrateur d'effectuer un ensemble de taches sur son panel personnel:

- Modifier un produit
- Supprimer un produit
- Consulter les enchères(en cours, fermée , gagnée)

- Supprimer un client
- Afficher les clients
- Supprimer, afficher les demandes
- Consulter les statistiques

4.2. Diagramme de classe :

Nous allons utilisée ce diagramme afin de représente la vue statique de notre conception, et afin de capturer les objets intervenant dans notre système et les interactions entre eux.

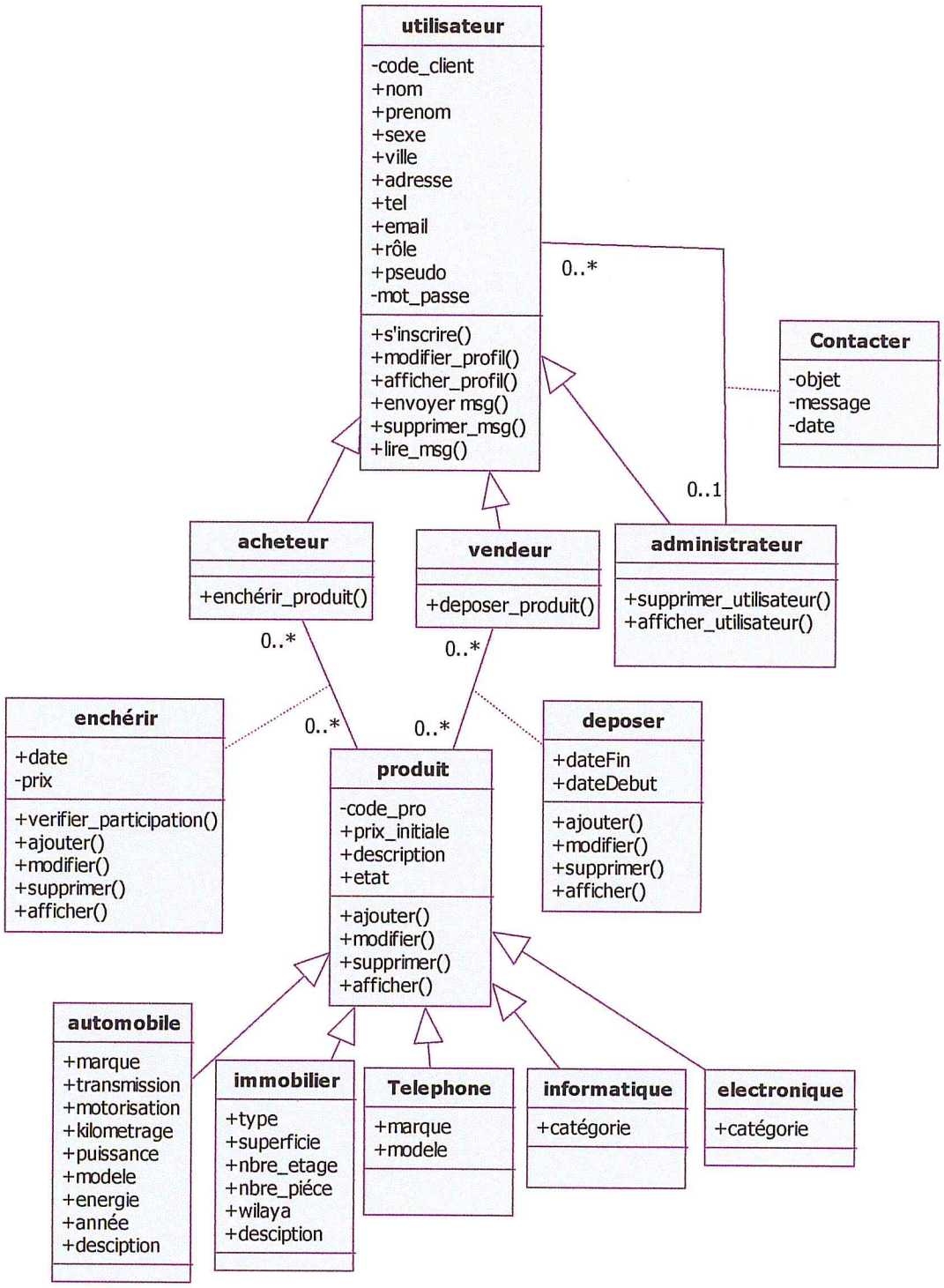


Figure 20:Diagramme de classe

4.2.1.Description des attributs et des opérations:

Classe utilisateur		
Cette classe représente l'utilisateur du site		
Attribut	**Type**	**Signification**
-code_client	String	Identifiant d'utilisateur.
+nom	String	Nom d'utilisateur..
+prénom	String	Prénom d'utilisateur.
+ sexe	String	Sexe d'utilisateur.
+ville	String	La ville d'utilisateur.
+ adresse	String	L'adresse d'utilisateur.
+ tel	String	Le téléphone d'utilisateur.
+ email	String	Email d'utilisateur.
+ pseudo	String	Le pseudo d'authentification
-mot passe	String	Le mot de passe d'authentification
Opération		**Signification**
+ s'inscrire ()		S'inscrire au site
+ modifier profil()		Modifier le profil
+ afficher profil()		afficher le profil
+ envoyer msg()		Envoyer un message
+ lire msg()		Lire un message
+ supprimer msg()		Supprimer un message

Tableau III.1:Description de la classe utilisateur

Classe acheteur	
Cette classe représente un acheteur qui est un utilisateur de notre système	
Opération	**Signification**
+ enchérir ()	Enchérir un produit(achat au enchère)

Tableau III.2:Description de la classe acheteur

Classe Vendeur	
Cette classe représente un vendeur qui est un utilisateur de notre système	
Opération	**Signification**
+ déposer_ produit ()	Déposer un produit au vente aux enchères

Tableau III.3:Description de la classe acheteur

Classe administrateur	
Cette classe représente un administrateur qui est un utilisateur de notre système	
Opération	**Signification**
+ supprimer utilisateur ()	Enchérir un produit(achat au enchères)
+ afficher utilisateurs ()	Enchérir un produit(achat au enchères)

Tableau III.4:Description de la classe administrateur

Classe contacter		
C'est une classe association entre la classe utilisateur et la classe administrateur		
Attribut	**Type**	**Signification**
+objet	String	L'objet de message
+ message	String	Le message a envoyer

+ date	Date	Date d'envoie du message

Tableau III.5:Description de la classe contacter

Classe produit		
Attribut	**Type**	**Signification**
-code pro	String	L'identifiant du produit
+prix-initiale	Float	Le prix initiale du produit a vendre
+ description	String	comporte les détail en plus
+état	String	L'état d'un produit :vendu, non vendu
Opération		**Signification**
+ ajouter()		Ajouter un produit
+ modifier()		Modifier un produit
+supprimer()		Supprimer un produit
+afficher()		Afficher un produit

Tableau III.6:Description de la classe produit

Classe enchérir		
Attribut	**Type**	**Signification**
+date	Date	La date de participation
-prix	Float	Le prix soumis pour le produit a acheter
Opération		**Signification**
+ ajouter()		Ajouter l'acheteur et le produit a l'enchère
+ modifier()		Modifier l'acheteur et le produit de l'enchère
+supprimer()		Supprimer l'acheteur et le produit a l'enchère
+afficher()		Afficher l'acheteur et le produit l'enchère
+ verifier_participation()		Vérifier si l'acheteur a déjà participer a l'enchère

Tableau III.7:Description de la classe enchérir

Classe déposer		
Attribut	**Type**	**Signification**
+date début	Date	La date de début d'enchère pour tel produit
+date fin	Date	La date de fin d'enchère pour tel produit
Opération		**Signification**
+ ajouter()		Ajouter le produit
+ modifier()		Modifier le produit
+supprimer()		Supprimer le produit
+afficher()		Afficher le produit

Tableau III.8:Description de la classe déposer

4.3. Diagrammes de séquence

Un diagramme de séquence est une série d'évènements ordonnés dans le temps, simulant une exécution particulière du système **[13].** Le temps y est représenté explicitement par une dimension verticale et s'écoule de haut en bas **[14].**

Nous allons représenter quelques diagrammes de séquence jugés important pour montrer la dynamique du système .

- Diagramme de séquence : enchérir un produit .
- Diagramme de séquence : modifier un produit
- Diagramme de séquence : déposer un produit

4.3.1 Diagramme de séquence : enchérir un produit

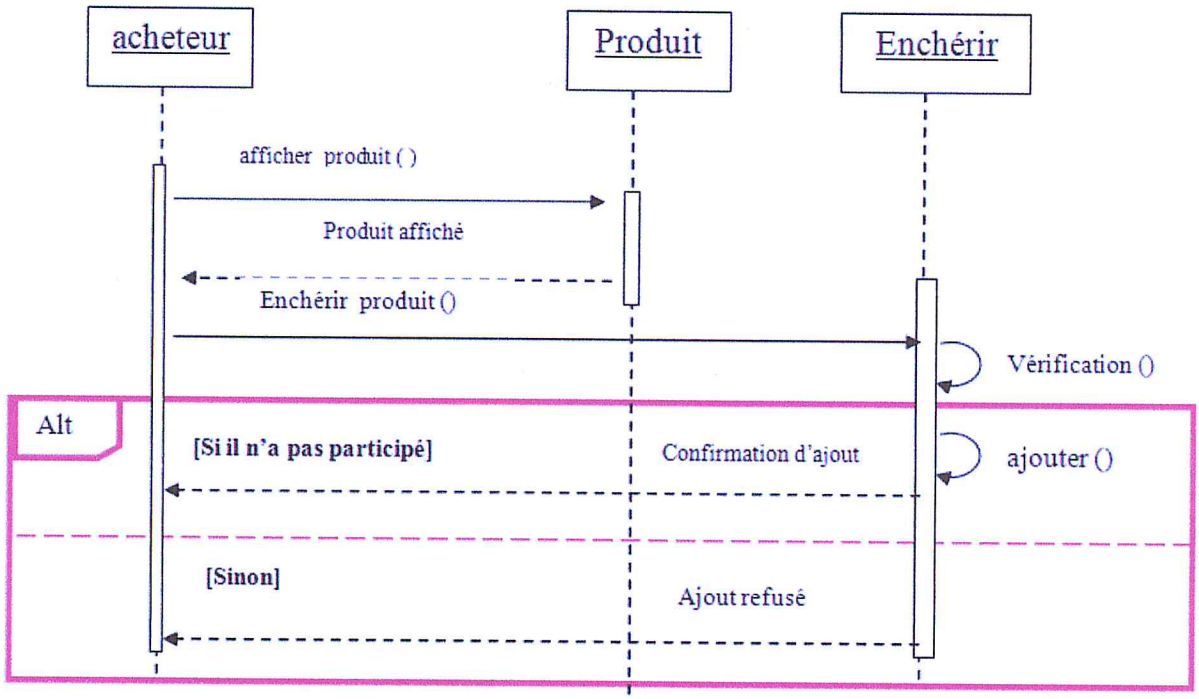


Figure 21:Diagramme de séquence enchérir un produit

4.3.2 Diagramme de séquence : modifier un produit

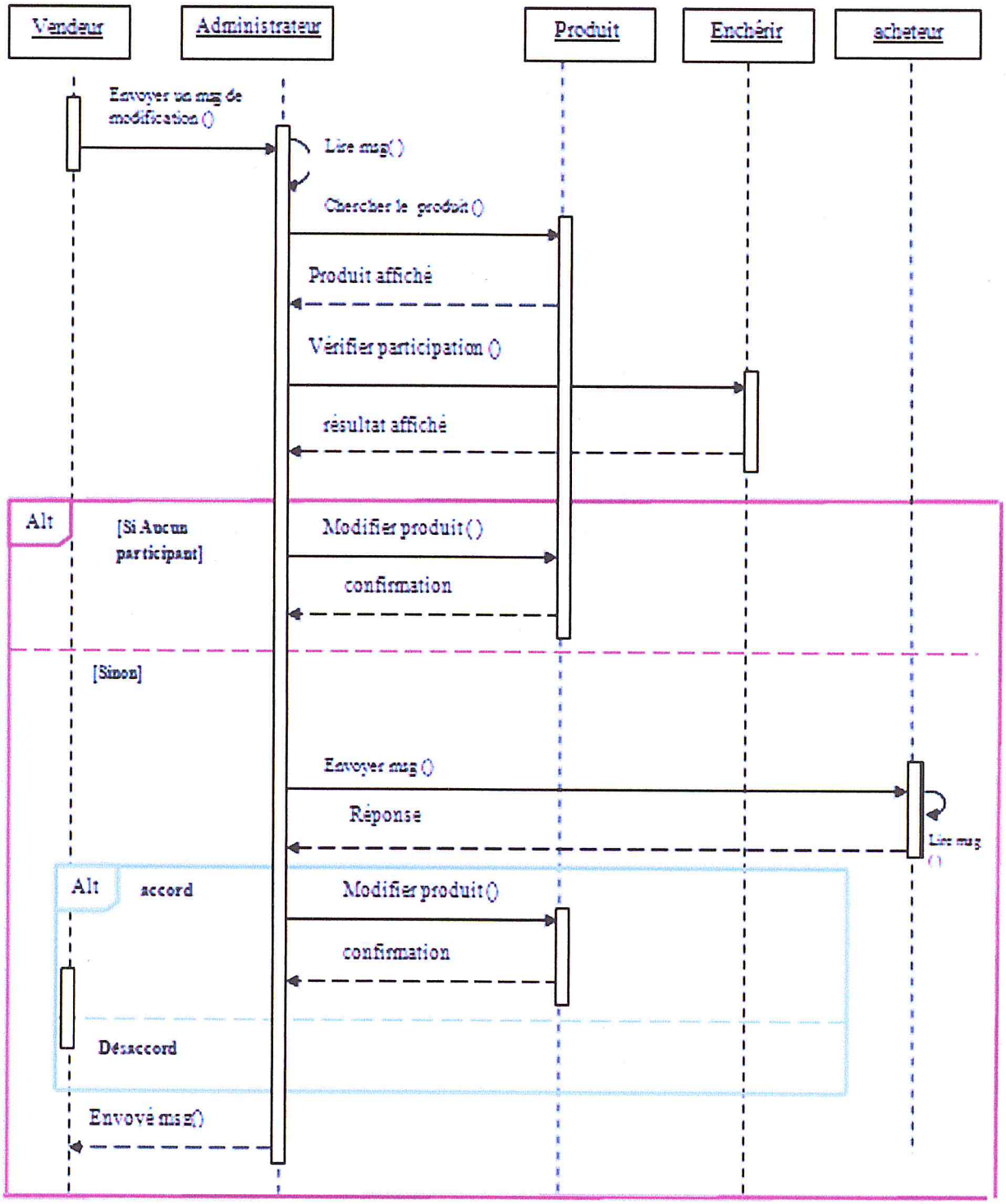


Figure 22 :Diagramme de séquence modifier un produit

4.3.3 Diagramme de séquence : déposer un produit

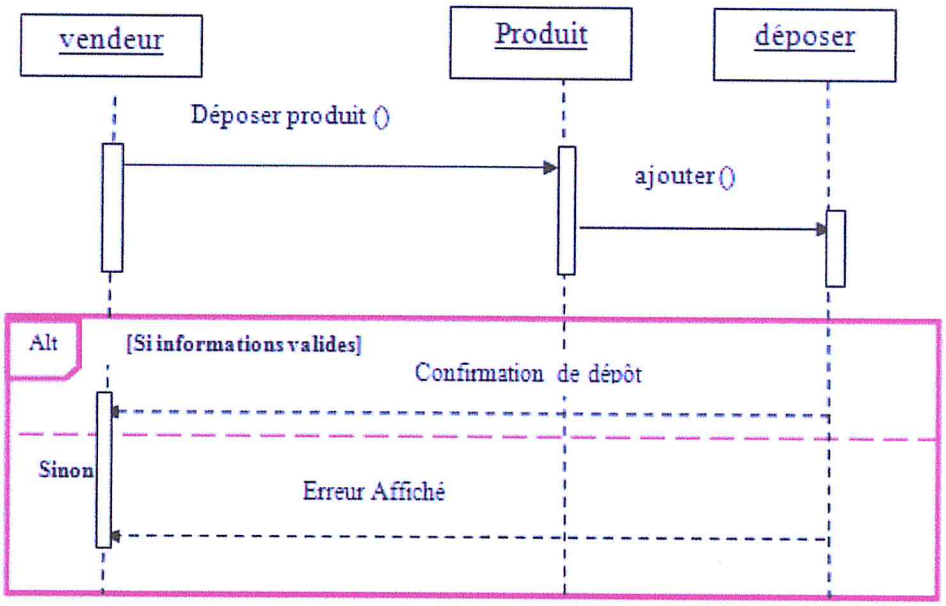


Figure23. :Diagramme de séquence déposer un produit

4.4. Diagramme d'activité :

Nous allons utilisé le diagramme d'activité pour montrer l'enchaînement des actions et décisions au sein d'une activité .

Nous allons représenter quelques diagrammes de séquence jugés important pour montrer la dynamique du système .

- Diagramme d'activité: enchérir un produit .
- Diagramme d'activité: modifier un produit
- Diagramme d'activité :déposer un produit
- Diagramme d'activité : inscription

4.4. 1.Diagramme d'activité enchérir un produit

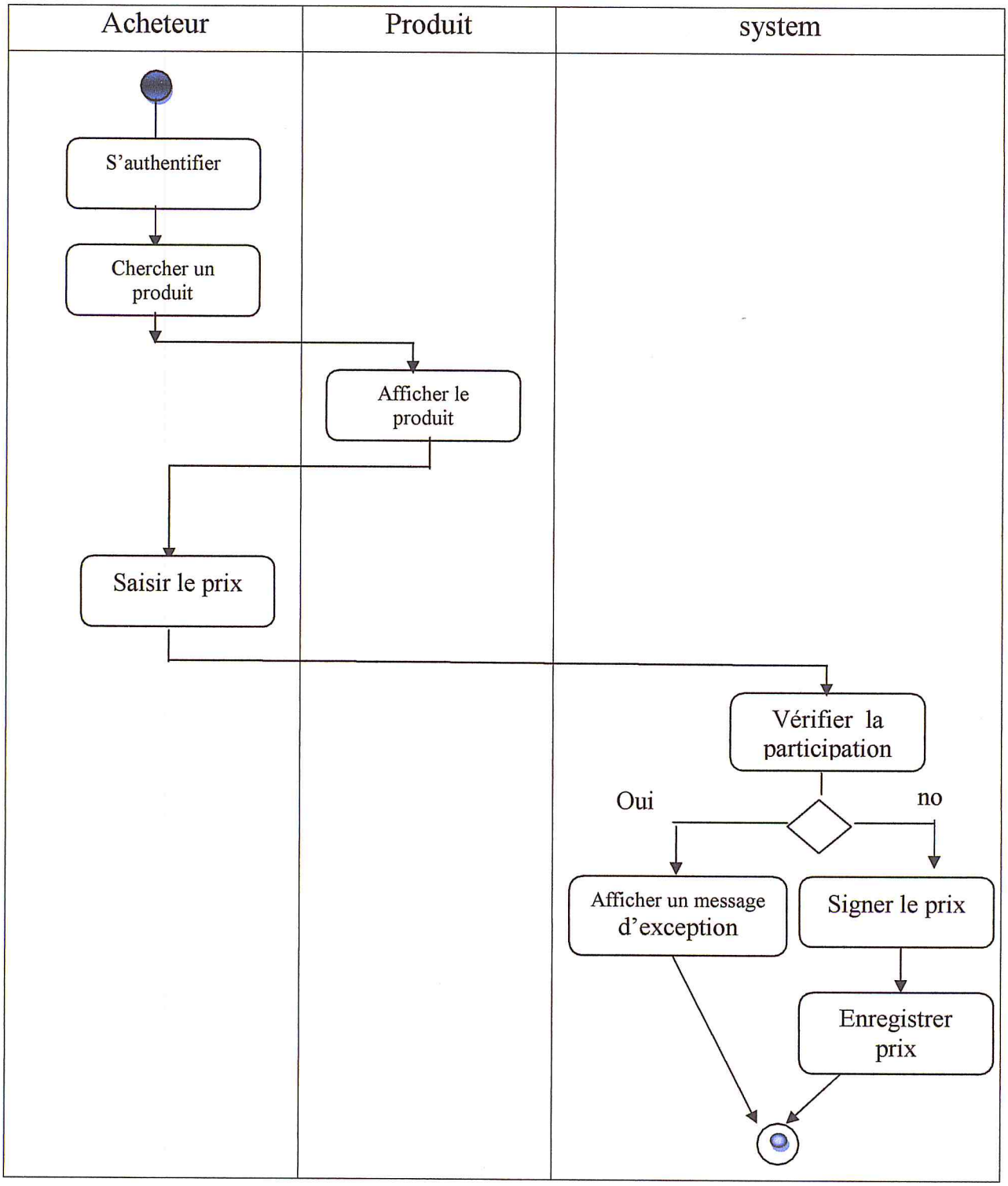


Figure 24 : Diagramme d'activité enchérir un produit

4.4. 2.Diagramme d'activité modification d' un produit

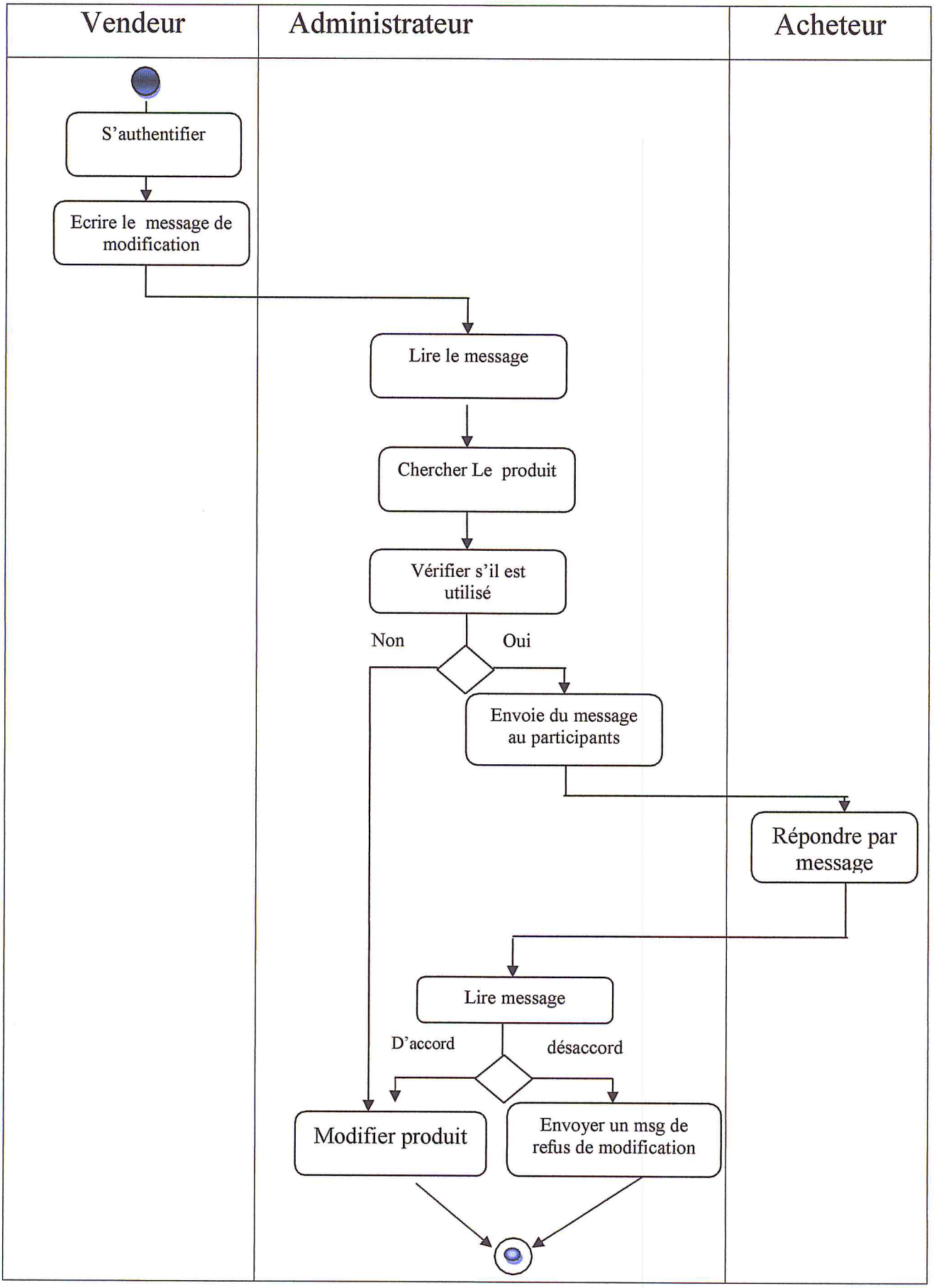

Vendeur
Administrateur
Acheteur
S'authentifier
Ecrire le message de modification
Lire le message
Chercher Le produit
Vérifier s'il est utilisé
Non
Oui
Envoie du message au participants
Répondre par message
Lire message
D'accord
désaccord
Modifier produit
Envoyer un msg de refus de modification

Fig20 : Diagramme d'activité modification d'un produit

4.4. 3.Diagramme d'activité inscription :

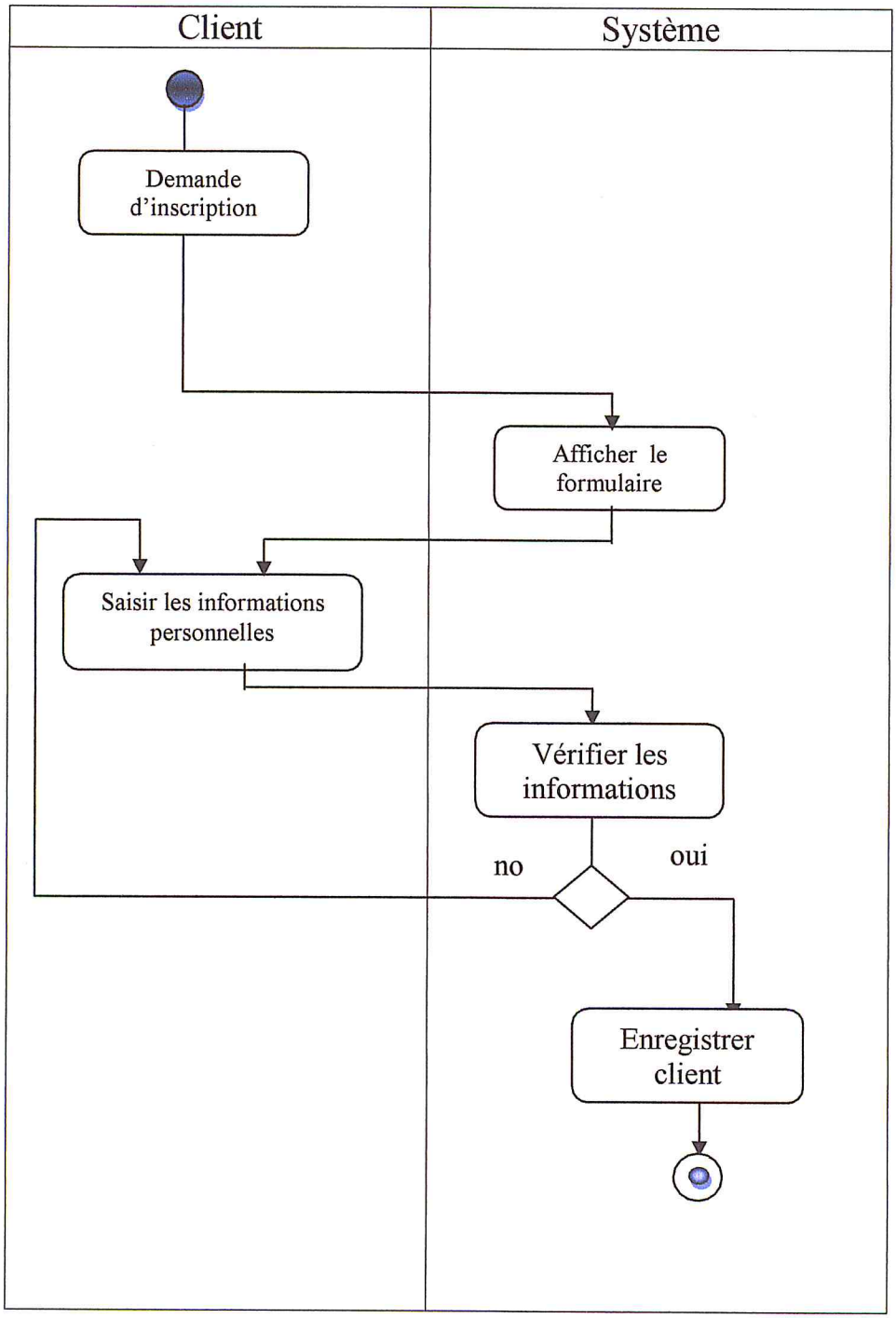


Figure 25: Diagramme de cas d'utilisation enchérissement d'un produit

4.4. 4.Diagramme d'activité déposer un produit :

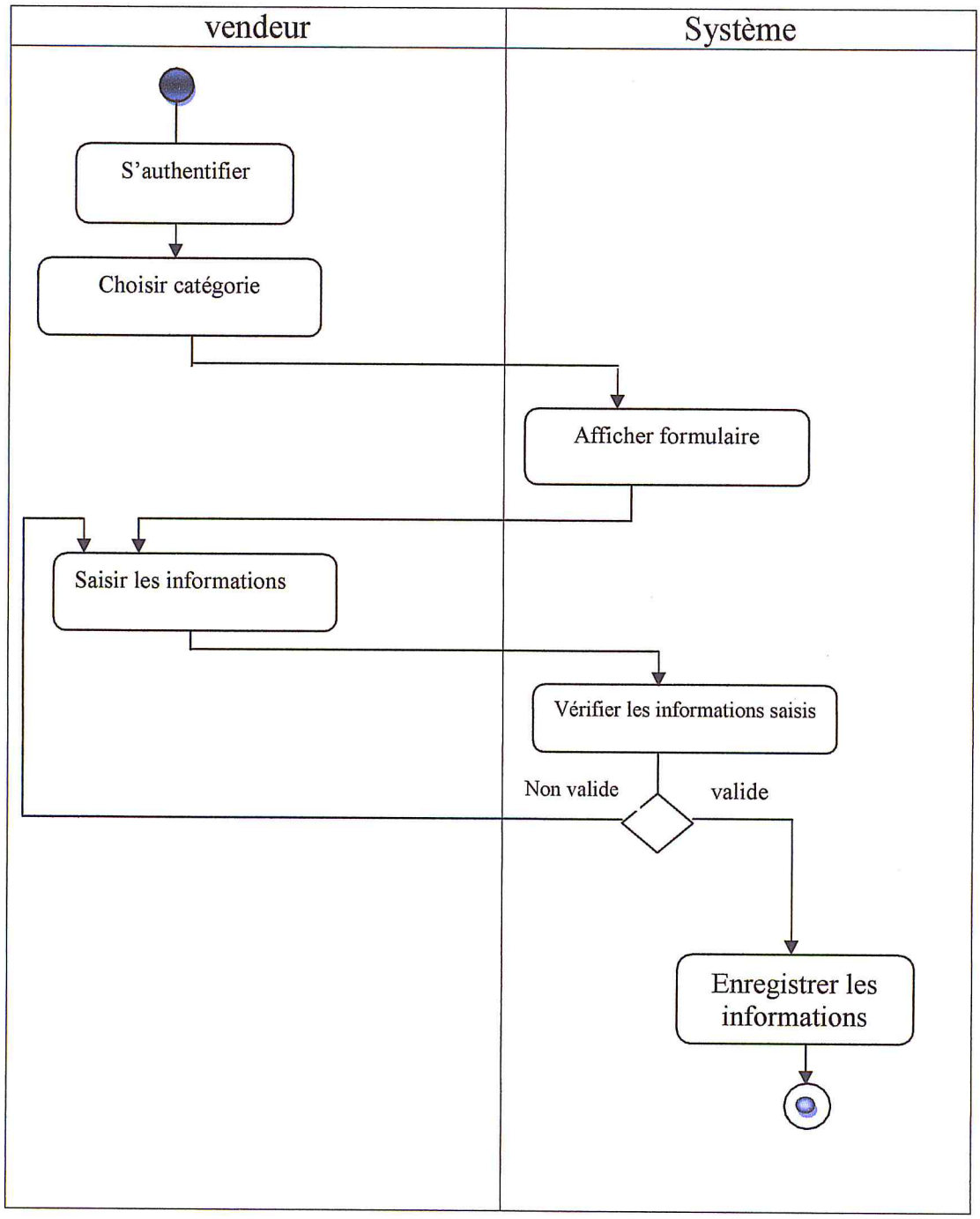


Figure 26: Diagramme d'activité le dépôt d'un produit

5.Conclusion

Dans ce chapitre, nous avons délimité les points à développer dans notre projet, à savoir, le développement d'une application web d'enchère et la sécurisation des transactions d'enchères.

Pour la conception de notre système nous avons présenté son architecture fonctionnelle puis sa modélisation avec le langage de modélisation UML.

A ce stade, nous pouvons passer à la réalisation de notre application, l'objet du chapitre suivant.

CHAPITRE 4

REALISATION

1. Introduction

Dans cette partie nous allons mettre en œuvre notre système tel qu'il est décrit dans la partie conception. Pour cela, nous justifions nos choix en matière d'environnement de développement. L'architecture technique. Le fonctionnement de notre application sera illustré.

2. Environnement de développement

Nous présentons dans cette section les outils que nous avons utilisés pour réaliser notre travail (serveur web, SGBD, langages de programmation) tout en justifiant nos choix.

Les logiciels que nous avons utilisés sont :

- Apache-Tomcat-6.0.32
- MySQL version 5.0.18
- Eclipse J2EE

2.1. Le serveur web Apache Tomcat [15]

Les serveurs web les plus populaires aujourd'hui sont : Apache, Microsoft IIS, Zeus et Sun One, etc. Nous avons choisit Apache pour les avantages suivants :

- Apache est gratuit.
- La configuration d'Apache s'effectue en modifiant ses fichiers de configuration au sein desquels des directives permettent de définir son comportement. Cette méthode de configuration lui procure une souplesse permettant à l'administrateur du serveur un contrôle sur les fonctionnalités et la sécurité offerte par Apache.
- Apache implémente SSL grâce au module mod-ssl et la bibliothèque Openssl (une boite à outils cryptographiques implémentant le protocole SSL) que nous avons utilisé pour les manipulations cryptographiques nécessaires.
- Tomcat a été écrit en langage Java. Il peut donc s'exécuter via la machine virtuelle Java sur n'importe quel système d'exploitation la supportant

Toutes ces caractéristiques nous ont permit l'utilisation facile de Openssl et configurer facilement notre serveur pour sécuriser notre application.

2.2. MYSQL [16]

Les SGBD libres et gratuits sont nombreux. MYSQL, mSQL, Postgres sont des exemples. Si nous avons choisit MYSQL, c'est plus pour des raisons de performances et fonctionnalités offertes. Nous citerons dans la suite ses principaux avantages :

- MYSQL est beaucoup moins complexes à installer et à administrer que d'autres systèmes.
- MYSQL permet des connexions multiples en même temps et utiliser différentes bases de données simultanément.
- MYSQL dispose d'un système de contrôle intégré qui interdit la consultation de données à ceux qui n'en ont pas l'autorisation.

2.3. Eclipse JEE

Java Platform, Enterprise Edition ou Java EE est une plate-forme largement utilisé pour la programmation web dans le langage de programmation Java. La plate-forme Java (Enterprise Edition) est différente de la plate-forme Java Standard Edition (Java SE) en ce qu'il ajoute les bibliothèques qui fournissent des fonctionnalités pour déployer à tolérance de pannes, distribués, à plusieurs niveaux du logiciel Java, largement basée sur des composants modulaires fonctionnant sur un serveur d'application**[17].**

3. Architecture technique de Dz Web Enchère :

Les communications entre l'administrateur, client et le serveur web se font avec le protocole HTTPS.

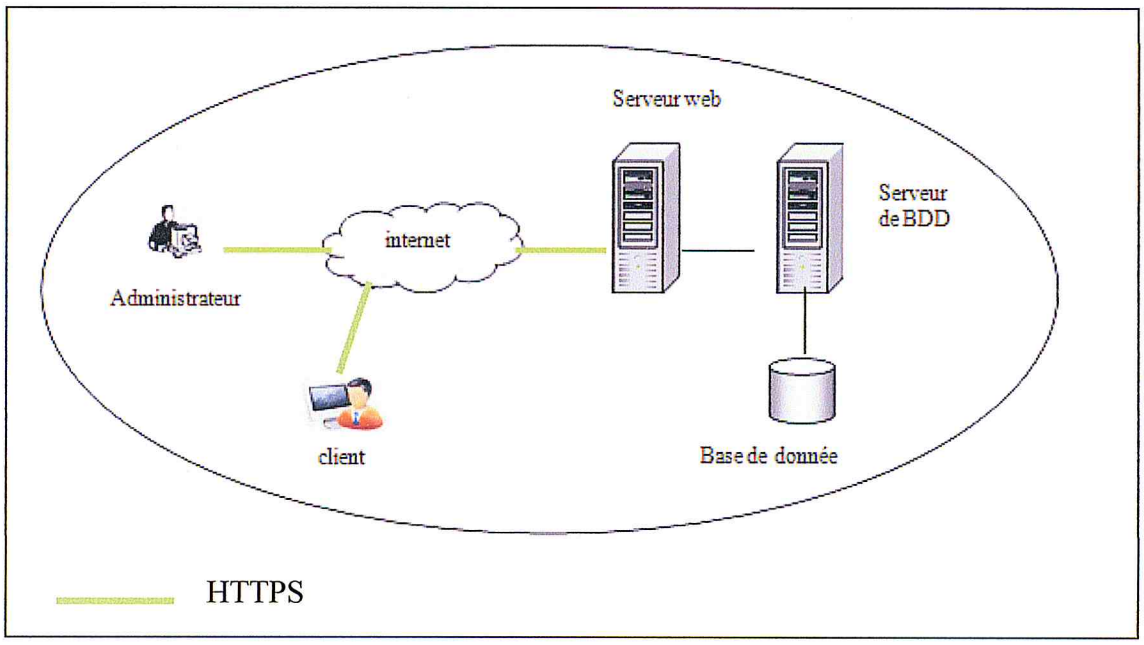


Figure 27: Architecture technique de dz web enchère

4. Fonctionnement de Dz web enchère

Dans ce qui suit, nous allons présenter certains aspects de notre système sous forme d'interfaces.

4.1. Page d'accueil :

Figure 28: page d'accueil de Dz web enchère

4.2. Les produits affichés par catégorie :

Nos produits sont classé par catégorie et ils sont affiché juste durant la phase d'enchères, quand la date fin d'enchère arrivera le produits est enlevé de la liste des produits et transféré vers la table archive pour un futur traitement

Exemple : La liste des produits de la catégorie « automobile » :

Figure 29: la liste des produits affiché par catégorie automobile

Le lien détail :
affiche tous le détail du produit avec un accès de participation a l'enchère

Figure 30 : détail du produit de la catégorie automobile

4.3. Interface de l'administrateur général

La figure suivante illustre l'interface propre à l'administrateur ainsi que les différentes fonctionnalités que lui offre la plate forme, il ya des fonctionnalité commune entre le client et l'administrateur comme :

- Modifier profil
- La messagerie

Figure 31 : Interface de l'administrateur

1- Clients : l'administrateur affiche la liste des clients avec le privilège de supprimer un client
2- Profil : espace de modification du profil
3- Messagerie : l'administrateur peut contacter ses clients par message , trouve la dans 3 sous menu (nouveau message, message reçu, les messages envoyé)
4- Gestion de catégorie : l'administrateur peut ajouter une nouvelle catégorie, modifier ou supprimer une catégorie.
5- Mes produits : tous les produits affichés par catégorie et avec tous les détails avec un accès

de suppression et de modification.

6- Les enchères gagnées : les produits vendus au enchères sont affiché seulement, avec le gagnant associé et le prix a payer par ce gagnant .ils sont classée par catégorie.

7- Les statistiques : des statistiques sur le taux de vendeurs, acheteurs sur le site, le produit le plus acheté, etc.

4.3.1 Les interfaces communes entre le client et l'administrateur :

4.3.1.1. Modifier profil :

Figure 32 : Interface de modification du profil

4. 3.1.2. Messagerie :

Envoyer un message :

Figure 33 : Interface « envoyer un message »

Message reçu :

Figure 34: Interface « message reçu »

4. 3.2. Interface de la liste des clients :

codeClient	Nom	prenom	Sexe	ville	Adresse	telephone	etat	Options
clt1	Batel	Sarra	Feminin	Alger	didouche mourad	12344444	En ligne	X
clt2	hachi	Zakia	Feminin	Blida	Blida	0000000	En ligne	X
clt3	chanane	aicha	Feminin	blida	boulvard	00000000	Hors ligne	X
clt4	Ziane	Hanane	Feminin	Blida	Bananier	000000	Hors ligne	X
clt7	Benstiti	imene	Feminin	Blida	Boulvard	9892333	Hors ligne	X
clt6	Ben m'hamed	Amani	Feminin	Blida	Zabana	23456	Hors ligne	X
clt5	Hamziou	Nesrine	Feminin	Blida	Ouled yaich	234567	Hors ligne	X
clt8	Boumaza	Abd el krim	Masculin	Blida	blida	234567	Hors ligne	X
clt9	Batel	Amine	Masculin	Blida	Ouled yaich	87654321	Hors ligne	X
clt10	Ben arbia	Akram	Masculin	Blida	diar el bahri	2345678	Hors Ligne	X

page -> [1]

Figure 35 : Interface « liste des clients »

4.3.3. Interface produits de la catégorie automobile :

Figure 36 : Interface de mes produits « les immobilier »

4.3.4. La liste des gagnants

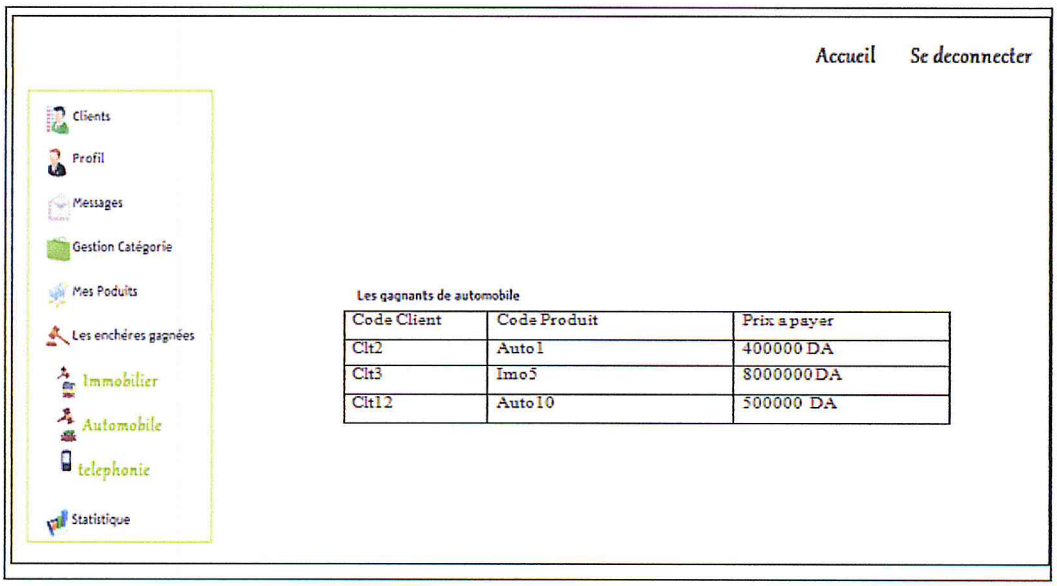


Figure 1 : l'interface des enchères gagnées

4.4. Interface de client

Cette interface qui décrit l'ensemble des fonctionnalités proposées au client est la plus importante dans notre site car c'est à partir d'elle que le client accède aux produits. La figure suivante illustre l'interface de client et ses fonctionnalités.

Figure 38 : Interface client

4.4.1. Interface du menu client

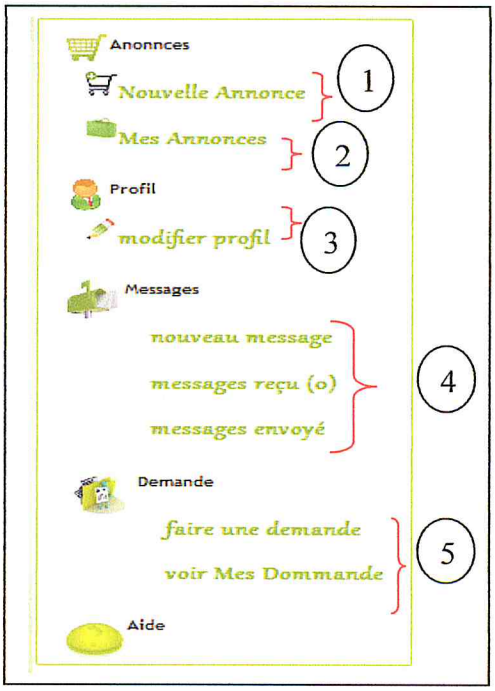


Figure 39 : menu client

Le menu afficher au client lui permet de :

1) déposer un produit :
2) consulter les produits déposés
3) modifier son profil
4) envoyer, recevoir, supprimer des messages
5) écrire une demande

4.4.2. Formulaire de la catégorie « immobilier » :

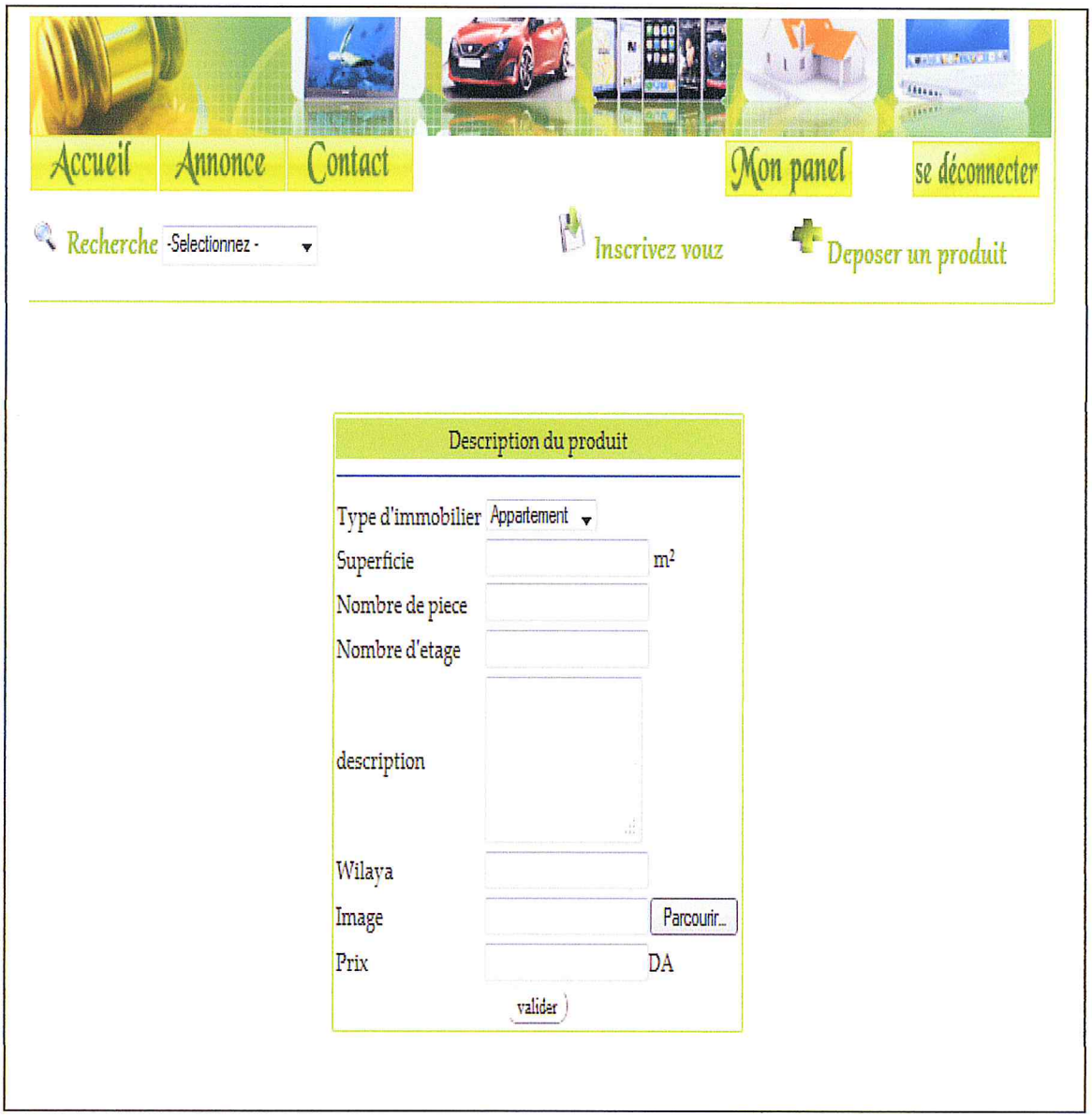


Figure 2 : formulaire d'ajout « catégorie immobilier »

4.4.3. Formulaire de la catégorie « automobile » :

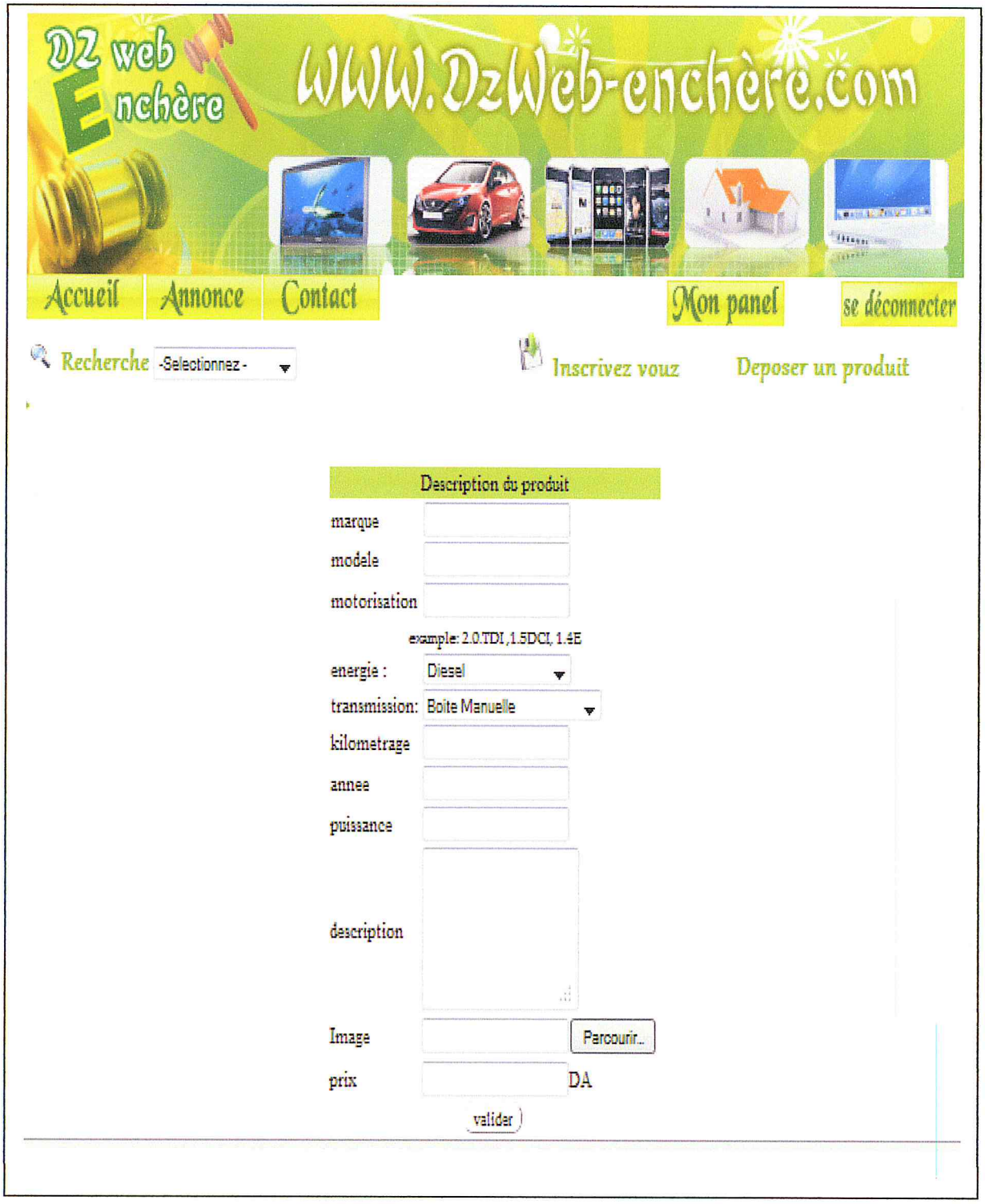


Figure 41 : formulaire d'ajout « catégorie automobile »

4.5. Connexion sécurisé :

Figure 42 : connexion sécurisé

5. Conclusion

Dans ce chapitre, nous avons justifié les choix des outils utilisés pour la réalisation de notre application. En suite, nous avons présenté quelques interfaces des différents acteurs et leurs fonctionnalités dans la plate forme en se basant sur le client.

Dans la suite de ce document, nous présenterons Quelques annexe

CONCLUSION GENERALE ET PERSPECTIVES

L'arrivée des technologies de l'information et de la communication a ouvert la voie à l'échange d'information, de biens et de services à distance. Le e-Commerce a pris naissance et est aujourd'hui en pleine expansion, les enchères sont l'une des formes d'achat et de vente. Cependant, les achats et la vente en ligne aux enchères sont menacés par des attaques visant à intercepter des informations confidentielles et d'usurper l'identité d'un utilisateur, etc. Pour expliciter ce contexte, nous avons fait une étude bibliographique englobant :

Un chapitre sur le e-commerce et les enchères sur lesquelles a porté notre application, tout en dégageant leurs besoins en sécurité.

Un chapitre sur la sécurité des échanges parcourant les notions de base de la cryptographie et le protocole SSL (Secure Socket Layer) a été mis en œuvre.

Nous sommes passées ensuite à la conception puis la réalisation de notre système. Nous avons développé un site web d'enchère en ligne; une application Web qui gère les transactions de vente et d'achat aux enchères en résolvant le problème de la triche supposée de l'administrateur.

Les objectifs fixés sont atteints. Cependant, des améliorations sur notre site web peuvent être rajoutées, nous citerons à titre d'exemples :

- Paiement en ligne
- Newsletter
- Ajouter d'autres formes de sécurité comme les injection SQL, HTML et JavaScript.

Pour évaluer le niveau de sécurité de notre système nous proposons de faire un audit de sécurité au futur.

ANNEXES

ANNEXE 1 : QUELQUES ALGORITHMES A CLE PUBLIQUE

Dans la cryptographie à clé publique (ou cryptographie asymétrique) chaque communicant utilisent deux clés, l'une est connue par tous (clé publique), l'autre n'est connue que par lui-même (clé privée). Le message crypté avec l'une ne peut être décrypté qu'avec l'autre [SER 03]. Les deux clés sont reliées mathématiquement entre elles de telle sorte qu'il est impossible de retrouver la clé privée en connaissant la clé publique.

1. L'algorithme RSA (Rivest Shamir Adleman)

Il existe différents algorithmes asymétriques. L'un des plus connus est le **RSA** (de ses concepteurs Rivest, Shamir et Adleman). Cet algorithme est très largement utilisé, par exemple dans les navigateurs pour les sites sécurisés et pour chiffrer les emails. Il est dans le domaine public.

1.2. Exemple :

Commençons par créer notre paire de clés:

- Prenons 2 nombres premiers au hasard: **p = 29, q = 37**
- On calcul **n = pq = 29 * 37 = 1073**
- On doit choisir **e** au hasard tel que **e** n'ai aucun facteur en commun avec **(p-1)(q-1)**:
- **(p-1)(q-1) = (29-1)(37-1) = 1008**
- On prend **e = 71**
- On choisit **d** tel que **71*d mod 1008 = 1**
- On trouve **d = 1079**
- On a maintenant nos clés :

  La clé publique est **(e,n) = (71,1073)** (=clé d'encryptage)

  La clé privée est **(d,n) = (1079,1073)** (=clé de décryptage)

On va encrypter le message '**HELLO**'. On va prendre le code ASCII de chaque caractère et on les met bout à bout:

$$\mathbf{m = 7269767679}$$

Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que **n**. **n** comporte 4 chiffres, on va donc découper notre message en blocs de 3 chiffres:

726 976 767 900

(on complète avec des zéros)

Ensuite on encrypte chacun de ces blocs:

$$726^{71} \bmod 1073 = 436$$
$$976^{71} \bmod 1073 = 822$$
$$767^{71} \bmod 1073 = 825$$
$$900^{71} \bmod 1073 = 552$$

Le message encrypté est **436 822 825 552**. On peut le décrypter avec d:

$$436^{1079} \bmod 1073 = 726$$
$$822^{1079} \bmod 1073 = 976$$
$$825^{1079} \bmod 1073 = 767$$
$$552^{1079} \bmod 1073 = 900$$

C'est à dire la suite de chiffre **726976767900**.

On retrouve notre message en clair **72 69 76 76 79** : '**HELLO**'.

1.3. Dans la pratique

Dans la pratique, ce n'est pas si simple à programmer:

- Il faut trouver de grands nombres premiers (ça peut être très long à calculer)
- Il faut obtenir des nombres premiers **p** et **q** *réellement* aléatoires (ce qui est loin d'être évident).
- On n'utilise pas de blocs aussi petits que dans l'exemple ci-dessus: il faut être capable de calculer des puissances et des modulos sur de très grand nombres.

En fait, on utilise jamais les algorithmes asymétriques pour chiffrer toutes les données, car ils sont trop longs à calculer : on chiffre les données avec un simple algorithme symétrique dont la clé est tirée au hasard, et c'est cette clé qu'on chiffre avec un algorithme asymétrique comme le RSA.

2. L'algorithme DSA (Digital Signature Algorithm)

Le DSA est un algorithme de signature numérique standardisé par le NIST aux États-Unis, du temps où le RSA était encore breveté. Une révision mineure a été publiée en 1996 (FIPS 186-1) et le standard a été amélioré en 2002.

Le processus de signature se fait en trois étapes :

- génération des clés
- signature du document
- vérification du document signé

2.1. Générations des clés

- Choisir un nombre premier p de L-bit, avec $512 \leq L \leq 1024$, et L est divisible par 64
- Choisir un nombre premier q de 160 bits, de telle façon que $p - 1 = qz$, avec z un entier
- Choisir h, avec $1 < h < p - 1$ de manière à ce que $g = h^z \bmod p > 1$
- Générer aléatoirement un x, avec $0 < x < q$
- Calculer $y = g^x \bmod p$
- La clé publique est (p, q, g, y). La clé privée est x

2.2. Signature

- Choisir un nombre aléatoire s, $1 < s < q$
- Calculer $s1 = (g^s \bmod p) \bmod q$
- Calculer $s2 = (\mathrm{H}(m) + s1*x)s^{-1} \bmod q$, où $\mathrm{H}(m)$ est le résultat d'un hachage cryptographique avec SHA-1 sur le message m
- La signature est $(s1,s2)$

2.3. Vérification

- Rejeter la signature si 0<s1<q ou 0<s2<q n'est pas verifié
- Calculer $w = (s2)^{-1} \pmod q$
- Calculer $u1 = \mathrm{H}(m)*w \pmod q$
- Calculer $u2 = s1*w \pmod q$
- Calculer $v = [g^{u1}*y^{u2} \bmod p] \bmod q$
- La signature est valide si $v = s1$

ANNEXE 2: UML

(UNIFIED MODELING LANGUAGE)

UML (Unified Modeling language) est un langage de modélisation graphique et textuel destiné à décrire des besoins, spécifier, documenter des systèmes et architectures logicielles et concevoir des solutions [12].

1. Les treize diagrammes UML

UML 2.0 s'articule autour de treize types de diagrammes, chacun d'eux étant dédié à la représentation des concepts particuliers d'un système logiciel. Ces types de diagrammes sont répartis en deux grands groupes : [12]

• **Six diagrammes structurels** (concerne la structure du système pris " au repos ")

- Diagramme de classes : Il montre les briques de base statiques : classes, associations, interfaces, attributs, opérations, généralisations, etc.
- Diagramme d'objets : Il montre les instances des éléments structurels et leurs liens à l'exécution.
- Diagramme de packages : Il montre l'organisation logique du modèle et les relations entre packages.
- Diagramme de structure composite : Il montre l'organisation interne d'un élément statique complexe.
- Diagramme de composants : Il montre des structures complexes, avec leurs interfaces fournies et requises.
- Diagramme de déploiement : Il montre le déploiement physique des « artefacts » sur les ressources matérielles.

• **Sept diagrammes comportementaux :** (concerne la dynamique de fonctionnement du système)

- Diagramme de cas d'utilisation : Il montre les interactions fonctionnelles entre les acteurs et le système à l'étude.
- Diagramme de vue d'ensemble des interactions : Il fusionne les diagrammes d'activité et de séquence pour combiner des fragments d'interaction.
- Diagramme de séquence : Il montre la séquence verticale des messages passés entre objets au sein d'une interaction.

- Diagramme de communication : Il montre la communication entre objets dans le plan au sein d'une interaction.
- Diagramme de temps : Il fusionne les diagrammes d'états et de séquence pour montrer l'évolution de l'état d'un objet au cours du temps.
- Diagramme d'activité : Il montre l'enchaînement des actions et décisions au sein d'une activité.
- Diagramme d'états : Il montre les différents états et transitions possibles des objets d'une classe.

Nous détaillons dans la suite les quatre diagrammes que nous avons utilisé pour modéliser notre application, à savoir le diagramme de cas d'utilisation, de séquence de classe et d'état transition.

2. Diagrammes de cas d'utilisation

La représentation par diagramme de cas d'utilisation permet de voir de façon simple les différents acteurs, comment est délimité le système, les fonctionnalités demandées au système, et les rôles des différents acteurs vis-à-vis du système [13].

Une phase de spécification des besoins doit précéder la modélisation par diagramme de cas d'utilisation. Elle doit décrire sans ambiguïté le système logiciel à développer [14].

2.1. Identification des acteurs

Les acteurs sont les utilisateurs extérieurs au système qui interagissent avec ce dernier [14]. Un acteur peut consulter et/ou modifier directement l'état du système en mettant et/ou en recevant les messages susceptible d'être porteur de données [13].

2.2. Identification des cas d'utilisation

Un cas d'utilisation est un ensemble de séquences d'actions réalisées par le système produisant un résultat observable intéressant pour un acteur particulier. Il permet de décrire ce que le futur système devra faire sans spécifier comment il le fera [13]

2.3. Représentation graphique

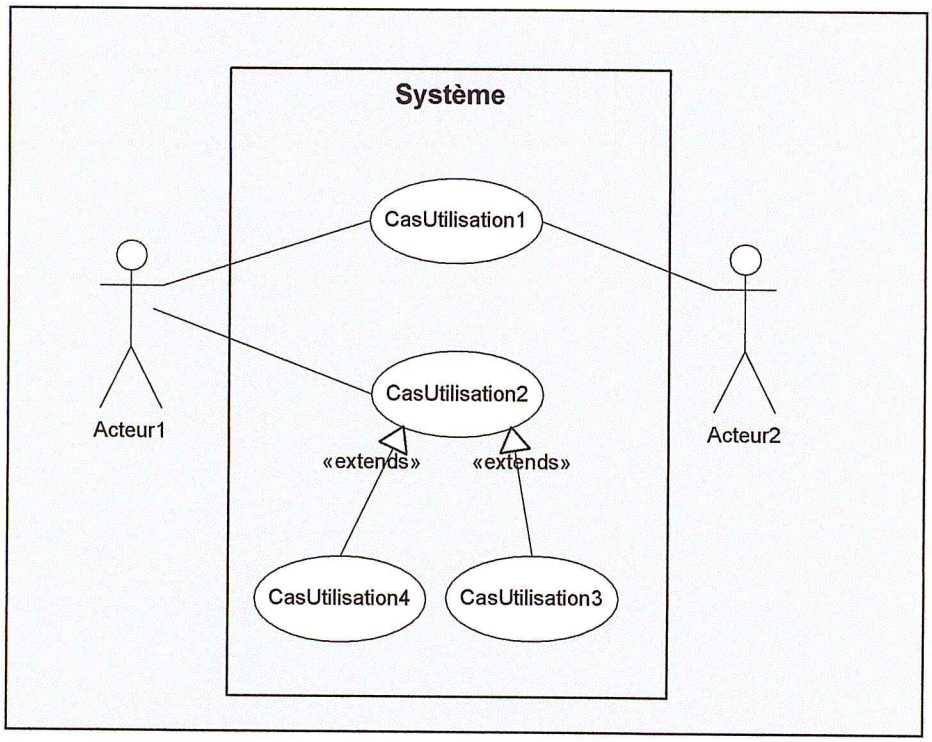


Figure 43: Représentation d'un diagramme de cas d'utilisation

Les associations entre acteurs et cas d'utilisation sont des relations qui signifient simplement « participe à » [14]

La relation « extends » indique que tout les cas d'utilisation fils sont des cas particuliers du cas utilisation père. Ils héritent de ces caractéristiques, c'est-à-dire qu'ils ont les mêmes liens avec les acteurs [14].

3. Diagrammes de séquence :

Un diagramme de séquence est une série d'évènements ordonnés dans le temps, simulant une exécution particulière du système [14]. Le temps y est représenté explicitement par une dimension verticale et s'écoule de haut en bas [13]

Dans un diagramme de séquence, les objets sont associés à **une ligne de vie**. Une ligne de vie est une représentation de l'existence d'un élément participant dans un diagramme de séquence.

L'élément de communication entre les objets est le **message**. Un message déclenche une activité dans l'objet destinataire. La réception d'un message provoque un événement dans l'objet récepteur. Leur ordre est donné par leurs positions sur la ligne de vie. Le concept de message unifie toutes les formes de communication entre objets (appel de procédure, événement discret, signal entre flots d'exécution ou interruption matérielle).

3.1. Représentation graphique :

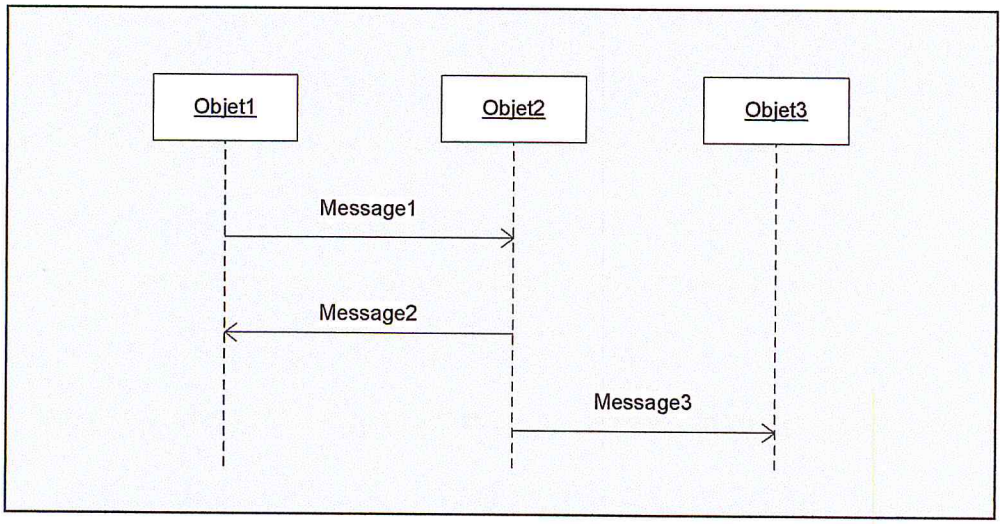


Figure 44: Représentation d'un diagramme de séquence

4. Diagrammes de classe

Le diagramme de classe représente les objets qui interviennent dans la résolution du problème ainsi que leurs associations [14].

Un digramme de classe est composé principalement de classes, d'associations entre classes et des classes d'association.

Classe : c'est une description d'un ensemble d'objets qui partage les mêmes attributs, opérations, méthodes, relations et contraintes. Une instance d'une classe est appelée objet.

Association : c'est une relation structurelle bidirectionnelle qui décrit un ensemble de liens entre différents éléments

Classe association : Une association peut être représentée par une classe appelée classe associative ou classe association. Utile par exemple, lorsque l'association a des attributs ou bien qu'on souhaite lui attacher des opérations. La classe association contient des attributs sans participer à des relations avec d'autres classes.

4.1. Représentation graphique

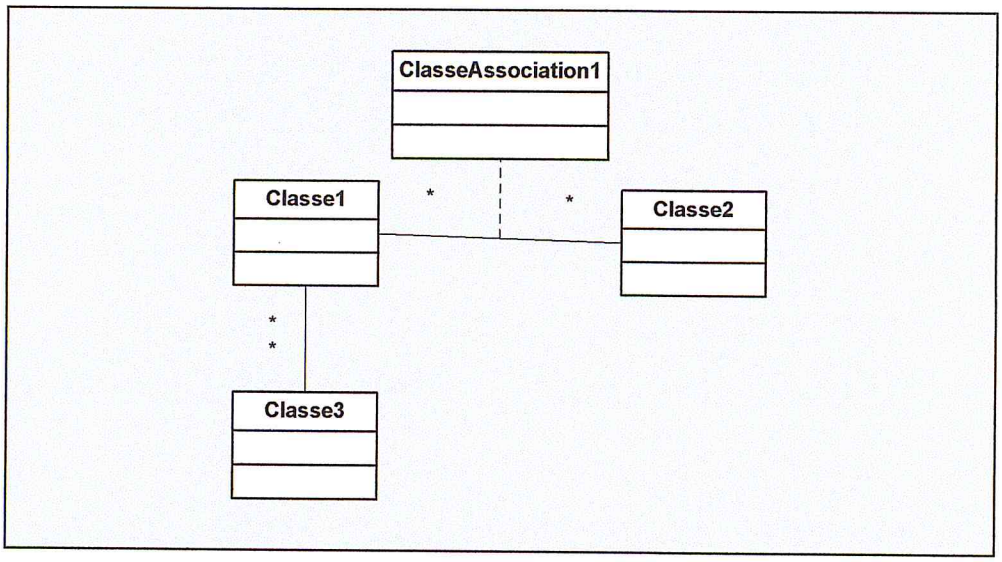


Figure 45: Représentation d'un diagramme de classe

ANNEXE 3 : LES CERTIFICATS NUMERIQUE

Certificat numérique et autorité de certification

Le principal avantage de la cryptographie à clé publique est qu'elle permet à des utilisateurs n'ayant pas d'accord de sécurité préalable d'échanger des messages de manière sûre. En effet, ces utilisateurs n'auront plus besoin d'échanger la clé secrète qui serais utilisée pour chiffrer les données échangées entre eux ; toutes les communications impliquent uniquement des clés publiques, et aucune clé privée n'est jamais transmise ou partagée.

Le problème posé par les systèmes cryptographiques à clé publique, est le fait que les utilisateurs doivent s'assurer qu'ils chiffrent leurs messages en utilisant la véritable clé publique de leur destinataire. Afin de confirmer l'appartenance d'une clé à son propriétaire supposé, on utilise le principe de certificats numériques qui font appel à une partie tiers appelé autorité de certification [4].

- **Certificat numérique**

Un certificat numérique fonctionne comme une pièce d'identité. C'est une information attachée à une clé publique, signé numériquement par une partie tierce de confiance (autorité de certification). L'objet de la signature est de garantir que les informations de certification ont été contrôlées et validées.

Les certificats numériques sont utilisés donc pour empêcher les tentatives de falsification de clé publique [4].

Le standard X509

Les certificats requièrent un format commun et ils s'appuient actuellement en grande partie sur le standard X.509.

X.509 est un standard de cryptographie de l'UIT (Union Internationale des Télécommunications). Il a été crée en 1988 [4].

Un certificat au format x509 version3 contient les données énumérées dans la figure suivante :

Version du certificat (certificate format version)
Numéro de série du certificat (certificate serial number)
Description de l'algorithme de signature de l'autorité de certification AC (signature algorithm identifier for certificate authority CA)
Nom de l'AC qui a généré le certificat (issuer x.500 name)
Période de validité (validity period)
Nom de l'utilisateur auquel appartient le certificat (Subject X.500 name)
Clé publique (subject public key)
Description de l'algorithme à utiliser avec la clé publique (subject public key information)
Identification possible de l'AC (optionnel) (issuer unique identifier)
Identification possible de l'utilisateur (optionnel) (subject unique identifier)
Extensions (optionnel)
Signature de l'AC (CA signature)

Figure 10 : Format d'un certificat X.509 V3 [4]

- **Autorité de certification AC**

L'autorité de certification est une partie tierce de confiance qui se porte garante de la validité de certificats numériques.

L'autorité de certification délivre, distribue les certificats numériques et elle les révoque en cas où les informations qu'ils contiennent ne sont plus valables **[4]**.

BIBLIOGRAPHIE

[1]	He, M., Jennings, N.R. and Leung, H., "On agent-mediated electronic commerce", IEEE Trans on Knowledge and Data Engineering,
[2]	SIDOUMOU, Med Redha., "APPLICATION DU E-BUSINESS EN ALGERIE ", , Université Saad Dahlab Blida (juin 2009)
[5]	Guttman, R.H., Moukas, A.G. and Maes, P., "Agent-Mediated electronic commerce: A survey", The knowledge engineering review
[6]	Cramton, P., Shoham, Y. and Steinberg, R., "An Overview of Combinatorial Auctions ACM SIGecom Exchanges, 7, (2007), 3-14.
[7]	Claude SERVIN,Réseaux et Télécommunications. Cours et exercices corrigés. Edition Dunod, 2003
[9]	Sécurité Optimale. Ressource d'expert. Livre anonyme. Edition S&SM, 1998
[10]	Sécurité optimale : le guide d'un ex-hacker pour protéger vos sites web et Votre réseau. Livre Anonyme. Edition CompusPress. 2001
[12]	UML2. Modéliser une application web. Livre de Pascal Roque. Edition Eyrolles 2006.
[13]	Intégrer UML dans vos projets. Livre de Nathalie Lopez, Jorge Migueis, Emmanuel Pichon. Edition Eyrolles, 1998.
[14]	Concevoir des applications web avec UML. Livre de Jim Conallen. Edition Eyrolles, 2000.

[15]	Apache professionnel. Peter WAINWRIGHT Edition Eyrolles, 2000
[16]	MYSQL, le serveur SQL de bases de données multi API Paul DUBOIS. Edition CompusPress, 2000
[19]	Sécurité optimale : le guide d'un ex-hacker pour protéger vos sites web et Votre réseau. Livre Anonyme. Edition CompusPress. 2001

WEBOGRAPHIE

[8]	http://www.scribd.com/doc/6910014/Le-Grand-Livre-De-Securite-Informatique, année : 2004.(Access date :02 April ,2011
[3]	http://securite.developper.com/fac/?page=dispo (Access date: 21 MARS, 2011)
[4]	http://www.hsc.fr/ressources/presentations/pki/img14.htm (Access date : 26 Mars, 2011) PKI et certificats Présentation de G.Labouret. 1999
[17]	http://en.wikipedia.org/wiki/Java_Platform,_Enterprise_Edition Année: August 2009, (Access date: 23/01/2011)