

UNIVERSITE ABOUBEKR BELKAID TLEMCEM

FACULTE DE TECHNOLOGIE



Département DEPARTEMENT DE GENIE ELECTRIQUE ET ELECTRONIQUE

Mémoire pour l'obtention de

**Diplôme de MASTER en Télécommunications**

Option **Réseaux Mobiles et Services**

Intitulé

***Solution E-business En Algérie  
(E-commerce)***

Présenté par

**Mr. BAGHDAD Othmane**

Soutenu en Juillet 2012 devant le jury composé de

**DJEMAI Abderrazak**

C.C. à l'Université de Tlemcen

**Président**

**HADJILA Mourad**

C.C. à l'Université de Tlemcen

**Examineur**

**IRID El-Hadj Sidi Mohamed**

M.A. à l'Université de Tlemcen

**Examineur**

**MERZOUGUI Rachid**

C.C. à l'Université de Tlemcen

**Encadreur**

**Année Universitaire : 2011-2012**

# Dédicaces

Je dédie ce mémoire

Aux êtres les plus chers à mon cœur, mes parents, symbole de bonté et de gentillesse, ceux *qui ont toujours été présents pour moi et qui m'ont toujours encouragé dans ma vie.*

A mes frères Salih et Younes à qui je leur souhaite beaucoup de réussite dans leur vie;

Ma gratitude la plus profonde à mes amis et frères présents, je cite en particulier :

- Abdelkrim BOUABDELLAH.
- Adil HABCHI.
- Ali BOUHEMAMA.
- Amine KHEMMAR.
- Chakir BABA-HAMED.
- Nabil BELMIR.

A tout le corps enseignant, administratif, et le personnel de la faculté des sciences et de l'ingénierat.

A vous qui lisez maintenant ce mémoire.

A tous ceux qui m'aiment & que j'aime.

**Othmane**

# Remerciements

Je remercie Dieu de m'avoir donné la santé et le courage afin de pouvoir réussir ce travail ;

Le travail présenté dans ce mémoire a été effectué au sein du laboratoire STIC de la faculté de technologie à l'université Abou Bekr Belkaïd Tlemcen.

Bien sûr, cette liste ne s'aurait être exhaustive, et je tiens par avance pour ceux que j'aurais oublié.

Tout d'abord, merci à Mr. MERZOUGUI Rachid, Mr. BENMOUSSAT Chemseddine et SEDJELMACI Hichem pour avoir encadré ce travail avec tant de compétence et de rigueur.

J'adresse tous mes remerciements à Mr DJEMAI Abderrazak de me faire l'honneur de présider le jury ; aussi j'adresse également mes remerciements les plus sincères à Mr. HADJILA MOURAD et Mr. IRID El-Hadj Sidi Mohamed membres du jury, je leurs suis très reconnaissantes pour le temps qu'ils ont consacré à lire et corrigé mon manuscrit.

Je ne saurais exprimer ma reconnaissance et ma gratitude à :

- MR. Nabil BELMIR Co-fondateur de ECHRI.
- MR Amine ABOURA Microsoft Student Partners.
- MR Le ministre des poste et télécommunications de nous avoir de nous avoir accueillies, et d'avoir été à notre écoute.
- MR Sofiane MELIANI notre infographe.

MERCI à tous ceux qui m'ont aidé à affiner et préciser ma démarche.

Je tiens à remercier toutes les personnes ayant permis l'accomplissement de ce mémoire.

## Chapitre 01

|  |    |
|--|----|
| Introduction :                                       | 2  |
| 1. Les réseaux de mobile                             | 2  |
| <i>TABLEAU 1 • Générations de réseaux de mobiles</i> | 2  |
| 1.1.GSM  | 2  |
| 1.2.GPRS   | 3  |
| 1.3.L'UMTS   | 5  |
| 1.4. Le HSDPA (3.5G)                                 | 6  |
| 1.5.Le HSUPA (3.75G)                                 | 6  |
| 1.6.Le LTE   | 6  |
| 2. Les réseaux sans-fil                              | 7  |
| 2.1.Les réseaux Wifi                                 | 8  |
| 2.2.Les réseaux WIMAX                                | 9  |
| 2.3.Les réseaux Ad-hoc                               | 10 |
| 3. Internet.....                                     | 12 |
| 3.1.Les générations du réseau internet :             | 12 |
| 3.2.Fonctionnement du réseau :                       | 13 |
| 3.2.1. Le serveur                                    | 13 |
| 3.2.2. Le client                                     | 13 |
| 3.2.3. L'architecture client/serveur                 | 13 |
| 3.3.Présentation du modèle TCP/IP                    | 13 |
| 3.3.1. Description du modèle                         | 14 |
| 3.3.2. La couche hôte réseau                         | 15 |
| 3.3.3. La couche internet                            | 16 |
| 3.3.4. La couche transport                           | 16 |
| 3.3.5. La couche application                         | 16 |
| 3.4.Les protocoles du réseau Internet                | 17 |
| 3.5.Les applications Internet                        | 17 |
| 4. Internet mobile                                   | 19 |
| 4.1.Les applications de l'internet mobile            | 20 |
| 4.1.1. Le WAP (Wireless Application Protocol)        | 20 |
| 4.1.2. Le I-mode                                     | 21 |
| 5. La passerelle WAP                                 | 21 |
| 5.1.Fonctionnalités de la Gateway WAP                | 22 |

|   |    |
|---|----|
| 6. Les serveurs .....   | 22 |
| 6.1.Serveur web : .....   | 22 |
| 6.2.Serveur de base de données .....                            | 22 |
| 6.3.Serveur dédié .....   | 23 |
| Conclusion .....  | 23 |
| Chapitre 02   |    |
| E-business & technique de sécurité .....                        | 25 |
| Introduction : .....  | 25 |
| Le E-business : .....   | 25 |
| I. Partie I : le commerce électronique : .....                  | 26 |
| 1. COMMERCE ELECTRONIQUE .....                                  | 26 |
| 1.1Introduction .....   | 26 |
| 1.2Historique .....   | 27 |
| 1.3Généralités sur l'e-commerce .....                           | 27 |
| 1.3.1 Qu'est ce que le E-Commerce? .....                        | 27 |
| 1.3.2 Pourquoi E-Commerce ? .....                               | 28 |
| 1.4Déroulement et Processus impliqués dans l'e-commerce : ..... | 28 |
| 1.5Fonctions de l'E-commerce : .....                            | 29 |
| 1.6Type d'échange B2C .....                                     | 30 |
| 1.7Stratégies dans le e-commerce du type B to C .....           | 30 |
| 1.7.1 Clic & Mortar .....                                       | 30 |
| 1.7.2 La vitrine commerciale .....                              | 30 |
| 1.7.3 Boutique (ou site marchand) .....                         | 30 |
| 1.7.4 Galerie en ligne .....                                    | 31 |
| 1.8Avantages et inconvénients du e-commerce type B to C .....   | 31 |
| 1.9 Les avantages .....   | 31 |
| 1.9.1 Pour l'entreprise : .....                                 | 31 |
| 1.9.2 Les facteurs d'incitation au E-commerce : .....           | 32 |
| 1.9.3 Pour les clients .....                                    | 32 |
| 1.10 Les inconvénients .....                                    | 33 |
| 1.10.1 Pour l'entreprise : .....                                | 33 |
| 1.10.2 Pour les clients .....                                   | 33 |
| 2. E-commerce en Algérie .....                                  | 33 |

|       |  |    |
|-------|--|----|
| 2.1   | Modèle actuel des échanges commerciaux .....                           | 33 |
| 2.2   | Intérêt économique du passage au e-commerce en Algérie .....           | 34 |
| 2.3   | Causes du retard de l'e-commerce en Algérie .....                      | 34 |
| 2.3.1 | <i>Système bancaire non compatible</i> .....                           | 34 |
| 2.3.2 | <i>La réglementation et la législation</i> .....                       | 35 |
| 2.3.3 | <i>Economie informelle</i> .....                                       | 35 |
| 2.3.4 | <i>Habitudes des consommateurs</i> .....                               | 35 |
|       | Conclusion .....   | 35 |
| II.   | Partie 2 : le E-paiement .....   | 36 |
|       | Introduction .....   | 36 |
| 1.    | Définitions .....  | 36 |
| 1.1   | Définition du paiement électronique (E-Paiement) .....                 | 36 |
| 1.2   | Définition du Terminal de Paiement Electronique .....                  | 37 |
| 1.2.1 | Fonctionnement .....   | 37 |
| 2.    | E-commerce et E-paiement .....   | 38 |
| 2.1   | Adaptation du paiement au contexte électronique .....                  | 38 |
| 2.2   | Moment du paiement .....   | 39 |
| 2.3   | Lieu du paiement .....   | 39 |
| 2.4   | Quittance .....  | 39 |
| 3.    | Moyens de paiement en ligne .....                                      | 40 |
| 3.1   | Payer par carte bancaire .....   | 40 |
| 3.2   | Payer par E-numéro de carte .....                                      | 40 |
| 3.3   | Payer sans carte bancaire .....  | 40 |
| 4.    | Contraintes attendues .....  | 40 |
|       | Conclusion .....   | 41 |
| III.  | Partie 03 : les techniques de Sécurité .....                           | 41 |
|       | Introduction .....   | 41 |
| 1.    | La sécurité et les types de risque dans le commerce électronique ..... | 41 |
| 1.1   | Risques de sécurité et de la vie privée : .....                        | 42 |
| 1.2   | Les risques de la plate forme .....                                    | 42 |
| 1.3   | Les risques des applications du logiciel .....                         | 42 |
| 3.    | Les techniques de sécurité de l'E-paiement .....                       | 43 |
| 3.1   | Chiffrement (ou cryptage) .....  | 43 |
| 3.1.1 | Type de Chiffrement .....  | 43 |

|  |    |
|--|----|
| 3.1.2 Efficacité de la méthode .....                       | 45 |
| 3.2 Signature numérique .....                              | 46 |
| 3.3 Infrastructure à clés publiques (PKI) .....            | 46 |
| 3.4 Certificat d'authentification .....                    | 47 |
| 3.4.1 Définition .....                                     | 47 |
| 3.4.2 Les informations du certificat .....                 | 47 |
| 3.4.3 L'utilisation des certificats .....                  | 48 |
| 3.4.4 Inconvénients de l'utilisation des certificats ..... | 48 |
| 3.5 Protocole de sécurité dans le paiement en ligne .....  | 49 |
| 3.5.1 Protocole SSL .....                                  | 49 |
| 3.5.2 Secure Electronic Transactions (SET) .....           | 51 |
| 3.5.3 3-D Secure .....                                     | 52 |
| 3.5.4 Protocole WTLS .....                                 | 53 |
| 3.5.5 Protocole SET .....                                  | 56 |
| 3.5.6 Le protocole HTTPS .....                             | 58 |
| Conclusion .....   | 58 |
| <b>Chapitre 03</b>   |    |
| 1. Benchmarking .....                                      | 60 |
| 1.1 Définition.....  | 60 |
| 1.2 Etude de l'offre du marché.....                        | 60 |
| 1.3 Analyse Comparative.....                               | 60 |
| 1.3.1 Analyse comparative E-commerce :                     | 60 |
| 1.3.2 Analyse comparative E-paiement .....                 | 61 |
| 2. Capture des besoins .....                               | 63 |
| 3. Notre solution .....                                    | 63 |
| 3.1 Un site internet promotionnel.....                     | 64 |
| 3.2 La solution de paiement électronique.....              | 64 |
| 4. Cahier de charge .....                                  | 66 |
| 4.1 Cahier pour site marchand.....                         | 66 |
| 4.1.1 Objectifs .....                                      | 66 |
| 1.1.1 Cible .....  | 67 |
| 1.1.2 Langues .....  | 67 |
| 1.1.3 Aspect et qualité du site .....                      | 67 |

|   |    |
|---|----|
| 1.1.4 Référencement .....   | 68 |
| 1.1.5 Version mobile du site .....                                  | 68 |
| 4.2 Cahier de charge RAHA PAY.....                                  | 68 |
| 4.2.1 Le module RAHAPAY .....                                       | 68 |
| 4.2.2 L'application mobile .....                                    | 68 |
| 5. RAHA PAY : comment ça marche .....                               | 69 |
| Conclusion .....  | 70 |
| <b>Chapitre 04</b>  |    |
| Introduction .....  | 72 |
| 1. Aperçu de notre solution à réaliser : .....                      | 72 |
| 2. La réalisation du site Web marchand : .....                      | 73 |
| 3. Réalisation du module paiement : .....                           | 74 |
| 4. Réalisation des carte de recharge pour RAHA PAY .....            | 74 |
| 5. Réalisation de l'application mobile .....                        | 75 |
| 5.1 Développement sur téléphone portable.....                       | 75 |
| 5.1.1 Qu'est ce que donc Windows Phone ? .....                      | 75 |
| 5.1.2 Les composants Windows phone .....                            | 75 |
| 5.1.3 Choix de Windows Phone : un PC dans le creux de la main ..... | 76 |
| 5.1.4 Condition du fonctionnement .....                             | 77 |
| 5.1.5 Interface de l'utilisateur final .....                        | 77 |
| 5.1.6 Exécution de l'application : .....                            | 77 |
| Conclusion .....  | 81 |

| Liste des figures | Titres  |
|-------------------|---|
| Figure 01         | Architecture du GSM                                       |
| Figure 02         | Architecture du GPRS                                      |
| Figure 03         | Réseau UMTS global  |
| Figure 04         | Principales normes des réseaux sans fil                   |
| Figure 05         | Architecture d'un réseau Wi-Fi                            |
| Figure 06         | Réseau WIMAX  |
| Figure 07         | Réseau Ad-hoc   |
| Figure 08         | Architecture d'internet                                   |
| Figure 09         | Modèle client/serveur.                                    |
| Figure 10         | Comparaison entre le modèle OSI et TCP/IP                 |
| Figure 11         | Environnement de l'Internet mobile                        |
| Figure 12         | Communication WAP   |
| Figure 13         | Architecture protocolaire WAP                             |
| Figure 14         | Les différents composants de l'E-commerce                 |
| Figure 15         | Les sept briques de l'E-commerce B to C                   |
| Figure 16         | Les facteurs d'incitation à l'E-commerce.                 |
| Figure 17         | Terminal de Paiement Electronique                         |
| Figure 18         | Schéma de déroulement d'un achat.                         |
| Figure 19         | Algorithme de chiffrement symétrique                      |
| Figure 20         | Algorithme de chiffrement Asymétrique                     |
| Figure 21         | Structure d'un certificat d'authentification              |
| Figure 22         | Etapes de la mise en œuvre d'un service HTTPS             |
| Figure 23         | Site sécurisé dont l'adresse possède le préfixe « https » |
| Figure 24         | Site web non sécurisé                                     |
| Figure 25         | Session sécurisé WTLS                                     |
| Figure 26         | Carte Interbancaire CIB.                                  |
| Figure 27         | Carte de paiement CCP.                                    |
| Figure 28         | Le logo de notre site marchand ECHRI                      |
| Figure 29         | Architecture de notre solution                            |
| Figure 30         | Capture d'écran de notre site WEB                         |
| Figure 31         | Module de paiement électronique                           |
| Figure 32         | carte de recharge RAHA PAY                                |
| Figure 33         | Pourcentage des systèmes d'exploitation mobile            |
| Figure 34         | Prévision pour les systèmes d'exploitation mobile         |
| Figure 35         | Lancement de l'application                                |
| Figure 36         | 1 <sup>er</sup> interface utilisation                     |
| Figure 37         | Services proposé par l'application                        |
| Figure 38         | Service de virement compte à compte                       |
| Figure 39         | La consultation du compte                                 |
| Figure 40         | Détails du compte   |

*Tableau01.Liste des figures.*

| <b>Liste des Tableaux</b> | <b>Titre</b>                               |
|---------------------------|--|
| Tableau01.                | Liste des figures.                         |
| Tableau02.                | Génération de réseaux de mobiles           |
| Tableau03.                | Principe de fonctionnement protocole WTLS. |
| Tableau04.                | Justification du choix de notre solution   |
| Tableau05.                | Liste des abréviations.                    |

| <b>Liste des abréviations</b> | <b>Significations</b>                                      |
|-------------------------------|--|
| E-Commerce                    | Commerce électronique                                      |
| E-Paiement                    | Paiement électronique                                      |
| B to C                        | Business to Customer                                       |
| M-Commerce                    | Mobile Commerce  |
| CIB                           | Carte Interbancaire  |
| TPE                           | Terminal de paiement électronique                          |
| CA                            | Certificat d'authentification                              |
| SSL                           | Protocole de sécurisation des échanges sur Internet        |
| VPN                           | Réseau privé virtuel                                       |
| SATIM                         | Société des transactions interbancaires et de la monétique |
| BDD                           | Base de données  |
| AES                           | Advanced Encryption Standard                               |
| AP                            | Access Point ou point d'accès                              |
| CEPT                          | Conférence européenne des Postes et Télécommunications     |
| NSDT                          | <b>Near Sound Data Transfer</b>                            |
| NFC                           | Near Field Communication                                   |

*Tableau05. Liste des abréviations*

## **INTRODUCTION GENERALE**

Les prévisions défient toutes les normes. Le marché du E-Commerce devra engranger quelques 13 000 milliards de dollars dans le monde d'ici 2012. Impensable! Le marché mondial du commerce électronique destiné au grand public (B2C) se chiffre actuellement à 1200 milliards de dollars. Le calcul des 13 000 milliards de dollars prévus à l'horizon 2012 est effectué en prenant en compte le E-Commerce B to B (entre professionnels) et B to C (vers le particulier).

Les chiffres vont encore crescendo concernant l'accès à Internet. 2 milliards de personnes, utilisent Internet, chose qui devrait augmenter, selon les spécialistes, le nombre des personnes qui seront appelées, par la force et l'évolution des choses, à effectuer des achats en ligne. L'on a prévu que d'ici à 2012, environ 1 milliard de personnes feront leurs courses sur Internet. Les choses semblent avancer à pas de géant atteignant un stade que l'on dénomme cyberconsommateurs impliquant aussi et surtout des créateurs d'entreprises. Le E-commerce, ce nouveau canal de vente et d'achat en ligne pourrait, selon les experts, connaître aussi une forte croissance en Algérie dans les années à venir. Il est vrai qu'actuellement l'on a recensé très peu de véritables sites de E-commerce en Algérie, capables d'effectuer des transactions de paiement en ligne. Le marché du E-commerce se limite actuellement en Algérie à des achats effectués par des étrangers munis d'une carte bancaire internationale.

Néanmoins, les prévisions des experts tablent sur un boom fulgurant qui serait l'effet de nombreux créateurs, particuliers ou entreprises qui se préparent à la révolution du E-commerce en Algérie. Des sites à vocation marchande avec vitrines et catalogues de produits, formulaires de commandes, réservations en ligne sont déjà mises en place en Algérie. C'est le tremplin. Un début prometteur. Ainsi, la tendance se précise de plus en plus. Elle commence à susciter l'intérêt des Institutions officielles nationales chargées des TIC, à savoir Algérie Poste et l'Autorité de régulation de la Poste et des Technologies de l'Information (ARPT). La filiale d'Algérie Télécom, qu'elle lancera le concept du commerce électronique en Algérie, via un projet pilote. Dans un premier temps, l'on met en avant les deux secteurs du Tourisme, celui de l'Artisanat et des PME-PMI comme case départ du E-commerce en Algérie.

La généralisation de l'accès à Internet Haut débit devrait donner un coup de pouce au projet E-commerce en Algérie. L'intérêt existe déjà et le premier pas est déjà effectué. Car, parler du commerce électronique conduit inévitablement à parler des TIC et plus particulièrement de l'Internet. La réforme en cours du système bancaire devrait aussi être le moteur propulseur car le développement du commerce électronique suppose la modernisation du système bancaire et la mise en place de nouvelles modalités de paiement, à l'instar du paiement à la carte, nécessaire pour le développement du E-commerce.

Une chose est sûr, il existe un énorme potentiel en Algérie afin d'entrer dans l'ère du E-business ou le commerce en ligne.

Vu que la technologie est au service de l'homme et non le contraire,

Vu que l'accès à internet n'est plus un luxe avec complément la téléphonie mobile,

Notre approche était avant tout de partir du client, de ses espérances, pour lui permettre de :

- acheter au bas prix, acheté mieux, être informé sur toutes les promotions qui existent, passer des commandes spécifiques.
- effectuer des micros achats sur internet, visualiser son compte, payer ses factures et d'autres transactions monétaire en utilisant son téléphone mobile ou internet sans pour autant se déplacer ou faire la queue toute en étant en voiture, au restaurant ...etc. et cela d'une manière fiable et sécurisée.

C'est dans cet état d'esprit, qu'on a décidé de mettre en place une solution de paiement mobile pour répondre aux besoins et satisfaire au mieux les exigences de nos clients et partenaires.

Le travail à réaliser est une première expérience en terme de projet, et ce afin de répondre aux objectifs suivants :

- Concevoir et réaliser une solution de E-commerce
- Intégrer un moyen de paiement électronique et l'adopter suivant les exigences de nos partenaires.
- Mettre en place la sécurité optimale nécessaire pour ce genre d'application contre les différentes vulnérabilités.
- Mettre en place un plan d'action pour généraliser notre système de paiement électronique comme solution alternatifs.

## **ORGANISATION DU DOCUMENT :**

Ce document est réparti en 4 chapitres:

- Le chapitre 1 « généralités technique»

Dans ce chapitre on présente les différents réseaux de téléphonie mobile ainsi, Internet et les principaux réseaux d'accès sans fil, ainsi que différents réseaux et architecture de système requise pour notre solution.

- Chapitre 02 « E-business & technique de sécurité »

On commence ce chapitre avec des définitions et du texte théorique dans le but de se familiariser avec les deux concepts abordés au cours du projet et qui sont : l'e-commerce et l'E-paiement. Et on finira par une présentation des différents moyens et d'aborder les dernières avancées techniques en matière de sécurité .

- Chapitre 03 « solution E-business »

Cette partie est consacrée à l'état de l'art selon (2) aspects :  
L'état de l'art marketing, où nous allons prendre connaissance du domaine bancaire et les différentes solutions E-business qui existent. Et on finira par proposer notre solution et imposer un cahier de charge pour sa réalisation.

- Chapitre 04 « réalisation »

Cette partie Dont nous allons présenter l'architecture générale et modulaire de notre solution. Nous parlerons également de la conception de l'application pour le M-commerce et le M-paiement, le site Web marchand ainsi que le module de paiement électronique intégré.

Et nous terminons ce mémoire avec une conclusion générale.

# Chapitre 1

## Généralités techniques

«La science nous incite donc à abandonner la recherche de la vérité absolue  
et à y substituer ce qu'on peut appeler la vérité "technique".» RUSSELL

## Introduction :

L'innovation technique et commerciale, multiplicité des offres, diversité des services et des produits ont largement contribué à l'essor de la téléphonie et de l'Internet au sein de la société industrielle moderne, permettant aux opérateurs de ce secteur de toucher un large public en satisfaisant des attentes aussi variées qu'évolutives.

Cependant, face à la quantité d'offres disponibles et à la technicité croissante des équipements, il est nécessaire pour chaque individu quelque soit ses compétences techniques, d'acquérir une quantité formidable d'informations pour exercer son choix. Comprendre le fonctionnement technique des offres, pour trouver une réponse à comment ça fonctionne, quelles sont ses limites....etc.

Un petit aperçu dans ce monde des nouvelles technologies, vous trouverez dans ce chapitre le vocabulaire et les définitions spécifiques aux différents outils techniques, afin que les mots GSM, WAP, GPRS, Serveur... n'aient plus de secrets pour vous.

### 1. Les réseaux de mobiles

Les équipements terminaux qui utilisent la voie hertzienne pour communiquer et qui peuvent se déplacer forment des réseaux de mobiles. Les réseaux sans fil, correspondant à des terminaux dont la mobilité l'objectif principal. [1]

| Génération                           | Réseau cellulaire  |
|--------------------------------------|--|
| 1 <sup>er</sup> génération           | NMT, R2000, AMPS, TACS                                   |
| 2 <sup>eme</sup> génération          | GSM, D-AMPS, PDC, PCS1800/1900, IS95A/IS41 et IS136/IS41 |
| 2 <sup>eme</sup> generation et demie | GPRS, IS95B  |
| 3 <sup>eme</sup> generation          | UMTS, W-CDMA, cdma2000, EDGE, DECT                       |
| 4 <sup>eme</sup> generation          | LTE  |

TABLEAU 2 • Générations de réseaux de mobiles

#### 1.1. GSM

Le GSM a été déployé au départ en Europe et partout dans le monde, à l'exception de l'Amérique, avant d'être adopté par plusieurs opérateurs américains.

La CEPT (Conférence européenne des Postes et Télécommunications) entreprend en 1970 d'établir une norme unique en matière de communication avec les mobiles. Dans le même temps, elle affecte une bande de 25 MHz dans la bande des 900 MHz pour réaliser un réseau cellulaire. Un groupe de travail, le groupe spécial mobile (GSM), est constitué pour réaliser ces études. En 1987, treize pays européens se mettent d'accord pour développer un réseau

GSM. En 1990, une adaptation de la bande des 1 800 MHz est mise en place sous le nom de DCS 1800 (Digital Communication System 1 800 MHz). À cette époque, l'ETSI remplace la CESTP pour finaliser la normalisation du GSM900 et du DCS 1800. De leur côté, les Américains reprennent une version du GSM dans la bande des 1 900 MHz, sous le nom de DCS1900. Les principes généraux du GSM sont les mêmes pour les trois adaptations.

Le GSM est un environnement complet, rassemblant l'interface air, mais aussi les interfaces entre le système radio et le système de commutation et l'interface utilisateur. Les appels sont contrôlés par la norme Q.931, déjà rencontrée dans le RNIS et le relais de trames.

La station mobile est constituée de deux éléments, le terminal portatif et la carte SIM. Cette carte à puce contient les caractéristiques de l'utilisateur et les éléments de son abonnement.

Le débit proposés sont limités dans les réseaux GM est de 14,4 Kbits/s.

Le GSM définit les relations entre les différents équipements qui constituent le réseau de mobiles :

- sous-système radio BSS ;
- sous-système réseau NSS (Network SubSystem), avec ses bases de données pour la Localisation des utilisateurs HLR et VLR ;
- relations entre les couches de protocoles et les entités du réseau ;
- interfaces entre sous-système radio (BSS) et sous-système réseau (NSS) ;
- itinérance (ROAMING). [2]

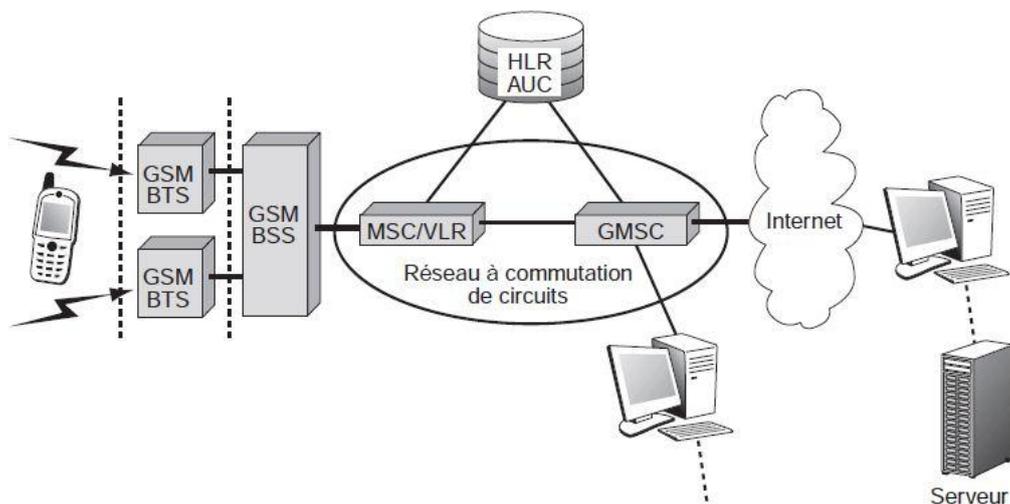


Figure 1. Architecture du GSM

## 1.2. GPRS

L'activité majeure de développement de la phase 2+, ou 2,5G, du GSM concerne le GPRS. Ce dernier incarne une nouvelle génération du standard GSM, rendant possible la prise en charge des applications de données à moyen débit dans le cadre de la mobilité. Il constitue en outre une transition vers la troisième génération, caractérisée par le passage d'un débit de 14,4 Kbit/s (9,6 Kbit/s utilisable) à un débit beaucoup plus important, pouvant être multiplié par 8 au maximum c'est à dire 171.2 Kbit/s théorique et 114 Kbit/s en pratique.

Le GPRS utilise la même infrastructure que le GSM mais avec un double réseau cœur, celui du GSM, c'est-à-dire d'un réseau à commutation de circuits, et celui d'un réseau à transfert de données. Si l'utilisateur téléphone, l'information transite par le réseau cœur de type circuit téléphonique. Si l'utilisateur émet des paquets, ces derniers sont acheminés par le réseau cœur de type paquet. Le réseau cœur utilise une technique de relais de trames. Nous ne considérons dans la suite que la partie paquet ajoutée au GSM.

Le terminal intègre les composants nécessaires au traitement de la parole téléphonique pour la numériser de façon plus ou moins compressée et se complète d'un modem, qui émet les paquets de l'utilisateur vers le réseau cœur paquet. La traversée de l'interface radio utilise les slots du TDMA qui ne sont pas utilisés par la parole téléphonique.

L'architecture du GPRS est illustrée à la figure suivante. Cette architecture est composée de divers types de nœuds :

- Les SGSN (Serving GPRS Support Node), qui sont des routeurs connectés à un ou plusieurs BSS.
- Les GGSN (Gateway GPRS Support Node), qui sont des routeurs acheminant le trafic vers des réseaux de données GPRS ou externes.

Le réseau GPRS possède deux plans, le plan utilisateur et le plan de signalisation. [3]

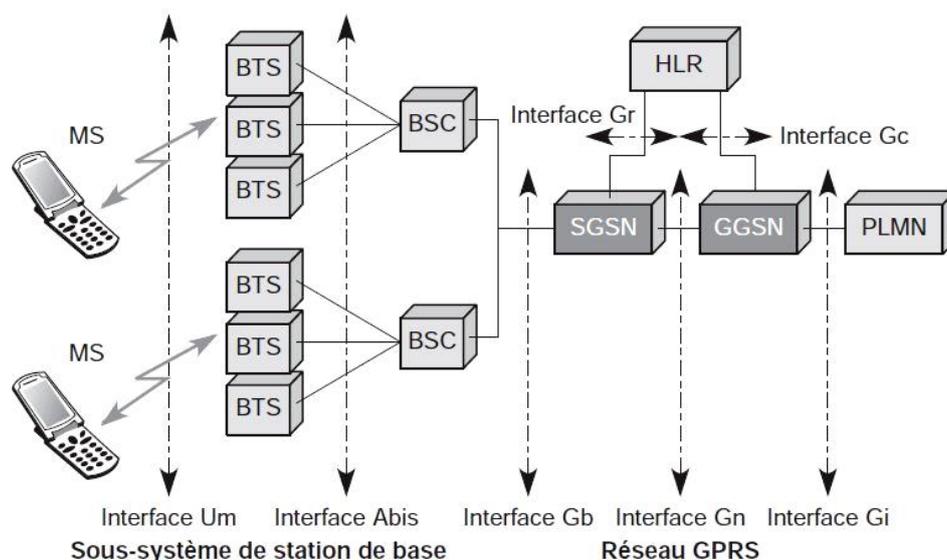


Figure 2. Architecture du GPRS.

### 1.3. L'UMTS

L'UMTS est l'une des technologies de téléphonie mobile de troisième génération (3G) standardisée par le 3GPP et constitue l'implémentation européenne des spécifications IMT-2000 de l'UIT pour les systèmes radio cellulaires 3G.

Le réseau UMTS est complémentaire aux réseaux GSM et GPRS. Le réseau GSM couvre les fonctionnalités nécessaires aux services de type voix en un mode circuit, le réseau GPRS apporte les premières fonctionnalités à la mise en place de services de type Data en mode paquets, et l'UMTS vient compléter ces deux réseaux par une offre de services Voix et Data complémentaire sur un mode paquet.

L'UMTS repose sur la technique d'accès multiple W-CDMA, ce qui permet d'obtenir un débit très important. Les fréquences allouées pour l'UMTS sont de l'ordre de GHz (1885-2025 MHz et 2110-2200 MHz).

Il permet théoriquement des débits de transfert de 1.920 Mbits/s, mais pratiquement les débits offerts par les opérateurs dépassent rarement 384 Kbits/s. Néanmoins, cette vitesse est nettement supérieure au débit de base GSM qui est de 9,6 kbit/s.

Grâce à sa vitesse accrue de transmission de données, l'UMTS ouvre la porte à des applications et services nouveaux. Cette génération permet en particulier de transférer dans des temps relativement courts des contenus multimédias tels que les images, les sons et la vidéo. Les nouveaux services concernent surtout l'aspect vidéo : Visiophonie, MMS Vidéo, Vidéo à la demande, Télévision.

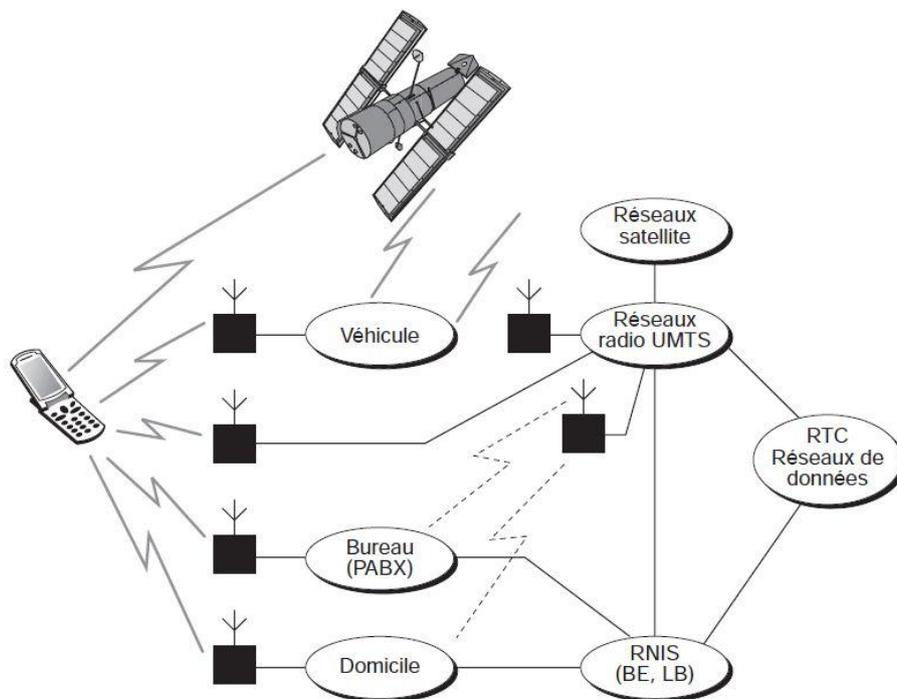


Figure 3. Réseau UMTS global

L'UMTS offre plusieurs services et application dont on peut citer quelle que uns :

- La visiophonie de poche : l'un des services les plus spectaculaires et les plus attendus des terminaux de la 3<sup>ème</sup> génération, ils permettent de voir l'interlocuteur avec lequel on discute.
- Fax et messagerie rapide : ces fonctions existent déjà sur certains téléphones de la 2<sup>ème</sup> génération, il n'est que perfectionné.
- Internet : outils privilégié, Internet représente à lui seul un des principaux atouts essentiels pour le développement, aussi bien auprès du grand public que des professionnels.
- Jeux multimédias : des jeux en solo ou en réseau sont disponible en couleurs et aux graphismes évolués.
- Application commerciale : la commande d'article ou la possibilité d'acheter des tickets, l'E-banking, le paiement de facture...etc.

#### 1.4. Le HSDPA (3.5G)

L'UMTS ne connaît pas un essor foudroyant, il impose des investissements énormes pour des débits finalement pas si éloignés de ceux du GPRS et se voit déjà rapidement remplacée par la nouvelle génération 3,5G, appelée HSDPA.

Cette nouvelle technologie annonce des débits pouvant aller au delà de 10 Mbits/s sur le lien descendant. Un autre avantage du HSDPA réside dans le fait qu'il puisse être déployé sans changer radicalement l'architecture de l'UMTS et permet du coup aux opérateurs de réaliser cette évolution à moindre coût. [4]

#### 1.5. Le HSUPA (3.75G)

Le HSUPA est une variante de HSDPA sur la voie montante. HSUPA présentée comme le successeur de HSDPA porte le débit montant (Uplink) à 5.8 Mbit/s théorique, le flux descendant (Downlink) étant de 14 Mbit/s comme en HSDPA. L'intérêt d'HSUPA est d'offrir la possibilité d'émettre vers d'autres mobiles, des images, des vidéos favorisant ainsi le développement de l'internet haut débit Mobile [5]

#### 1.6. Le LTE

LTE, ou Long Term Evolution, recouvre un ensemble de technologies amenées à prendre la suite des réseaux mobiles 3,5G (HSPA). Plus performante, avec une architecture tendant vers le tout-IP, elle prépare l'avènement du concept " broadband everywhere ".

L'actualité de la technologie **LTE** (*Long Term Evolution*), l'une des techniques en cours de validation en vue de faire évoluer les réseaux mobiles vers des débits toujours plus importants, s'est accélérée depuis 2007 avec la formation d'un groupement d'industriels (opérateurs, équipementiers, fabricants de terminaux) au sein de la **LSTI** (*LTE / SAE Trial Initiative*).

Cette LSTI a pour but de valider les expérimentations techniques qui permettront de pousser LTE au rang de standard. Confrontée au Mobile Wimax et à l'UMB (*Ultra Mobile Broadband*), LTE a cependant l'avantage d'avoir reçu le soutien d'une grande partie de

l'industrie-mobile.

Avec des débits de **100 Mbit/s descendants et 50 Mbit/s montants**, ce nouveau type de réseau mobile, qui a commencé à exister en Asie et en Europe dans 2 à 3 ans.

Ce qui se prépare aujourd'hui en coulisses annonce de grandes révolutions d'usages à venir avec une architecture réseau utilisant le protocole **TCP/IP** et des terminaux mobiles toujours plus tourné vers l'Internet et ses services. [6]

## 2. Les réseaux sans-fil

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer de place tout en restant connecté. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base, appelées points d'accès, ou AP (Access Point). Les communications entre points d'accès peuvent être hertziennes ou par câble. Les débits de ces réseaux se comptent en mégabits par seconde, voire en dizaines de mégabits par seconde. Plusieurs gammes de produits sont actuellement commercialisées.

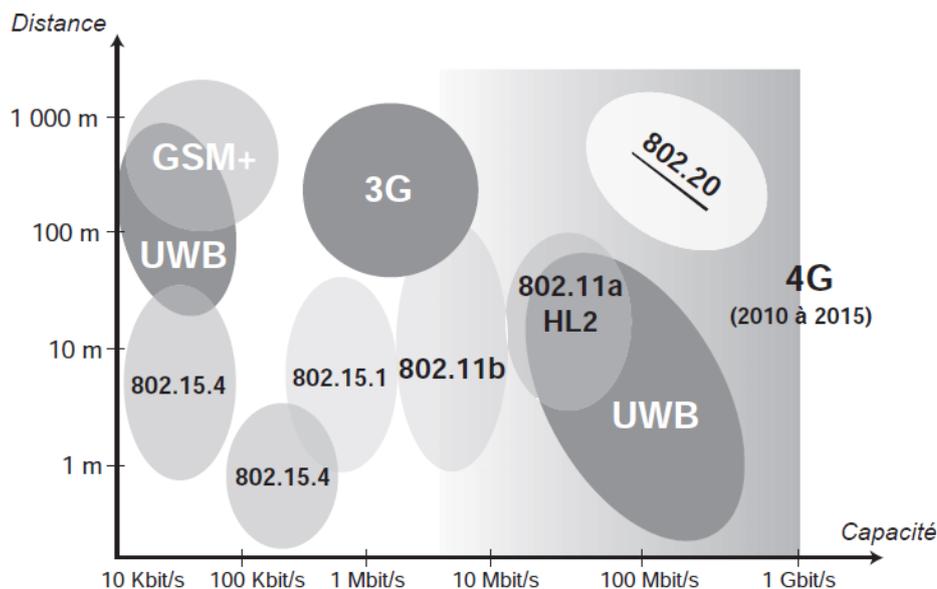


Figure 4 : Principales normes des réseaux sans fil

On va présenter les principaux réseaux de connexion sans fil.

### 2.1. Les réseaux WIFI

Wi-Fi suggère la contraction de Wireless Fidelity, par analogie au terme Hi-Fi, WI-FI est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11). Un réseau Wi-Fi permet de relier sans fil plusieurs appareils informatiques (ordinateur, routeur, décodeur Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.

Les normes IEEE 802.11 (ISO/CEI 8802-11), qui sont utilisées internationalement, décrivent les caractéristiques d'un réseau local sans fil (WLAN). La marque déposée

«Wi-Fi» correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance (« Wireless Ethernet Compatibility Alliance », WECA), organisme ayant pour mission de spécifier l'interopérabilité entre les matériels répondant à la norme 802.11 et de vendre le label « Wi-Fi » aux matériels répondant à leurs spécifications. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification (c'est du moins le cas en France, en Espagne, au Canada, en Tunisie...). Ainsi, un réseau Wi-Fi est en réalité un réseau répondant à la norme 802.11. Dans d'autres pays (en Allemagne, aux États-Unis par exemple) de tels réseaux sont correctement nommés WLAN (Wireless LAN).

Grâce aux normes Wi-Fi, il est possible de créer des réseaux locaux sans fil à haut débit. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA), des objets communicants ou même des périphériques à une liaison haut débit (de 11 Mbit/s théoriques ou 6 Mbit/s réels en 802.11b à 54 Mbit/s théoriques ou environ 25 Mbit/s réels en 802.11a ou 802.11g et 600 Mbit/s théoriques pour le 802.11n) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres).

Ainsi, des fournisseurs d'accès à Internet peuvent établir un réseau Wi-Fi connecté à Internet dans une zone à forte concentration d'utilisateurs (gare, aéroport, hôtel, train...). Ces zones ou point d'accès sont appelées bornes Wi-Fi ou points d'accès Wi-Fi ou « hot spots ».

Les iBooks d'Apple furent, en 1999, les premiers ordinateurs à proposer un équipement Wi-Fi intégré (sous le nom d'AirPort), bientôt suivis par le reste de la gamme. Les autres ordinateurs commencent ensuite à être vendus avec des cartes Wi-Fi intégrées tandis que les autres doivent s'équiper d'une carte externe adaptée (PCMCIA, USB, Compact Flash, SD, PCI, Mini PCI, etc.). À partir de 2003, on voit aussi apparaître des ordinateurs portables intégrant la plateforme Centrino, qui permet une intégration simplifiée du Wi-Fi. [7]

Il y'a différents normes Wi-Fi on peut citer : 802.11 (A, B, C, D, E, G, H, I, IR, J, N, S)

La norme 802.11g est la plus répandue dans le commerce actuellement. Elle offre un haut débit (54 Mbit/s théoriques, 25 Mbit/s réels) sur la bande de fréquences des 2,4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. Cette aptitude permet aux nouveaux équipements de proposer le 802.11g tout en restant compatibles avec les réseaux existants qui sont souvent encore en 802.11b. Le principe est le même que celui de la norme 802.11a puisqu'on utilise ici 52 canaux de sous-porteuses radio mais cette fois dans la bande de fréquences des 2,4 GHz. Ces sous-porteuses permettent une modulation OFDM autorisant de plus haut débit que les modulations classiques BPSk, QPSK ou QAM utilisé par la norme 802.11g.

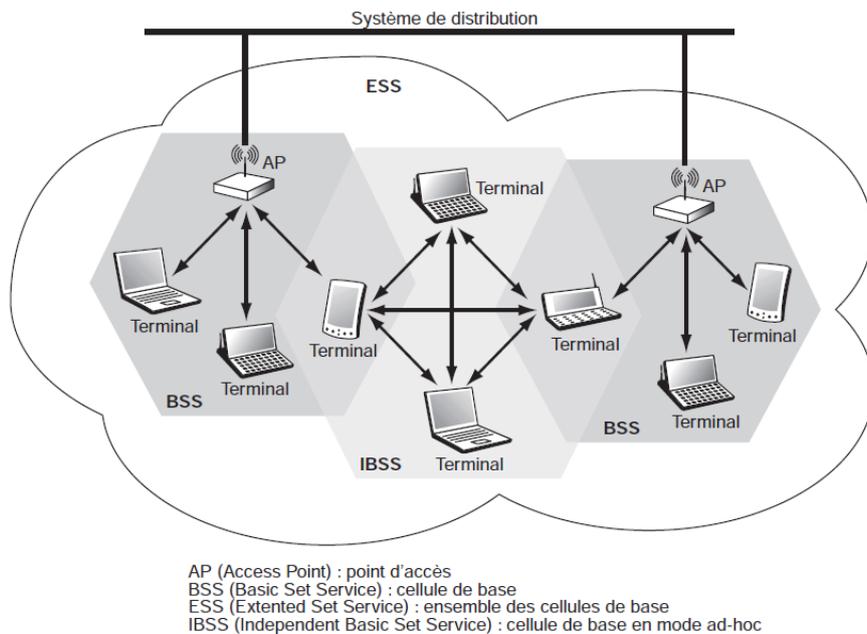


Figure 5. Architecture d'un réseau Wi-Fi

## 2.2. Les réseaux WIMAX

L'initiative Wimax est partie de l'idée de développer des liaisons hertziennes concurrentes des techniques xDSL terrestres. Après de longues années d'hésitation, le vrai démarrage de cette technologie a été favorisé par l'arrivée de la norme IEEE 802.16.

Avant de décrire brièvement cette norme, nous avons représenté un exemple de son utilisation à la figure suivante :

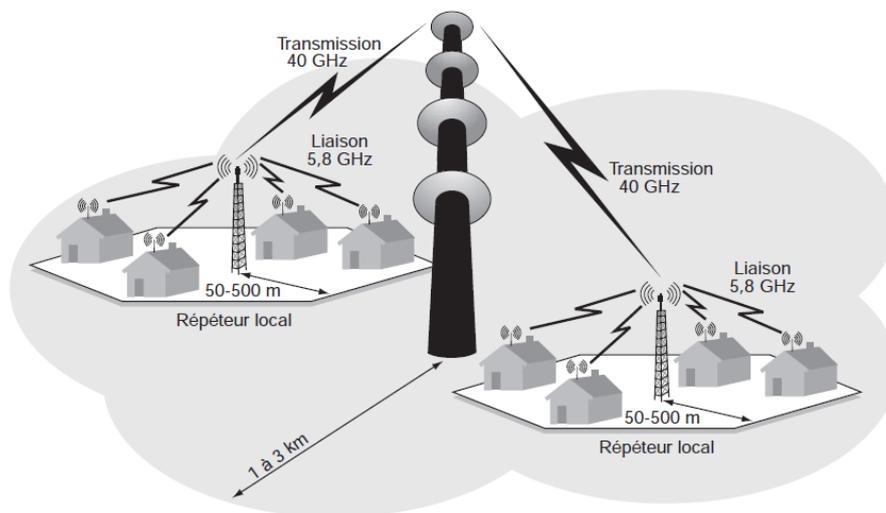


Figure 6. Réseau WIMAX

À partir d'une antenne d'opérateur, plusieurs répéteurs propagent les signaux vers des maisons individuelles, leur donnant accès à la téléphonie et à l'équivalent d'une connexion xDSL. Sur la figure, la connexion à l'utilisateur se fait en deux temps, en passant par un répéteur. Il est tout à fait possible d'avoir une liaison directe entre l'utilisateur et l'antenne de l'opérateur.

Le groupe de travail 802.16 a mis en place des sous-groupes pour s'attaquer à des problèmes distincts. Le groupe de travail de base a normalisé un accès métropolitain dans la bande des 10-66 GHz, avec une vue directe entre les antennes et un protocole point-à-point. Finalisée en 2001, cette norme a été complétée par les extensions 802.16c, en 2002, qui introduit les profils système Wimax, et 802.16d, en 2004, qui apporte des correctifs, ainsi que les éléments nécessaires à une compatibilité avec la future extension 802.16e.

Une autre extension, 802.16a, sortie en 2003, concerne la bande de 2 à 11 GHz et la possibilité d'utiliser des protocoles multipoint en plus de l'environnement point-à-point de base.

802.16e a pour objectif d'étendre Wimax à des machines terminales mobiles, impliquant donc la possibilité de réaliser des connexions xDSL vers des mobiles. Les fréquences utilisées se situeront entre 2 et 6 GHz.

Les différences entre ces normes et extensions et 802.11 sont nombreuses. D'abord, la portée est beaucoup plus grande, puisqu'elle peut dépasser 10 km, contre quelques dizaines ou centaines de mètres pour Wi-Fi. La technologie 802.16 est en outre moins sensible aux effets multi trajet et pénètre mieux à l'intérieur des bâtiments. Elle est de surcroît mieux conçue pour assurer le passage à l'échelle sur de grandes surfaces. Pour un canal de 20 MHz, Wimax permet enfin de faire passer un peu plus de débit, avec une meilleure qualité de service. En contre partie, les avantages de Wi-Fi résident dans son faible prix de revient, la forte réutilisation des fréquences qu'il permet et sa reconnaissance à peu près partout dans le monde. [8]

### 2.3. Les réseaux Ad-hoc

Une autre grande catégorie de réseaux est constituée par les réseaux ad-hoc, dans lesquels l'infrastructure n'est composée que des stations elles-mêmes. Ces dernières acceptent de jouer le rôle de routeur pour permettre le passage de l'information d'un terminal vers un autre, sans que ces terminaux soient reliés directement.

Un réseau ad-hoc est illustré à la figure suivante :

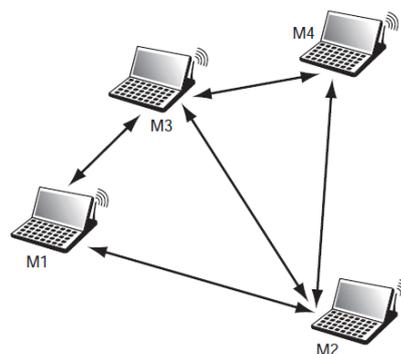


Figure 7. Réseau Ad-hoc

Contrairement aux apparences, les réseaux ad-hoc datent de plusieurs dizaines d'années. Ils visent à réaliser un environnement de communication qui se déploie sans autre infrastructure

que les mobiles eux-mêmes. En d'autres termes, les mobiles peuvent jouer le rôle de passerelle pour permettre une communication d'un mobile à un autre.

Deux mobiles trop éloignés l'un de l'autre pour communiquer directement peuvent trouver un mobile intermédiaire capable de jouer le rôle de relais.

La difficulté majeure engendrée par ce type de réseau provient de la définition même de topologie du réseau : comment déterminer quels sont les nœuds voisins et comment aller d'un nœud vers un autre nœud ? Deux solutions extrêmes peuvent être comparées. La première est celle d'un réseau ad-hoc dans lequel tous les nœuds peuvent communiquer avec tous les autres, impliquant une longue portée des émetteurs. Dans la seconde solution, au contraire, la portée hertzienne est la plus courte possible : pour effectuer une communication entre deux nœuds, il faut généralement passer par plusieurs machines intermédiaires. L'avantage de la première solution est la sécurité de la transmission, puisqu'on peut aller directement de l'émetteur au récepteur, sans dépendre d'un équipement intermédiaire. Le débit du réseau est minimal, les fréquences ne pouvant être réutilisées.

Dans le second cas, si un terminal tombe en panne ou est éteint, le réseau peut se couper en deux sous-réseaux distincts, sans communication de l'un à l'autre. Bien évidemment, dans ce cas, le débit global est optimisé, puisqu'il peut y avoir une forte réutilisation des fréquences. [9]

Les avantages des réseaux ad-hoc sont leurs extensions très simples, leur couverture physique et leur coût. Toutefois, pour en bénéficier pleinement, un certain nombre d'écueils sont à surmonter, telle la qualité de service et de sécurité, du fait de la mobilité des nœuds.

### 3. Internet

À la fin des années 60, le Département américain de la Défense décide de réaliser un grand réseau à partir d'une multitude de petits réseaux, tous différents, qui commencent à foisonner un peu partout en Amérique du Nord. Il a fallu trouver le moyen de faire coexister ces réseaux et de leur donner une visibilité extérieure, la même pour tous les utilisateurs. D'où l'appellation d'*Inter Network* (inter réseau), abrégée en Internet, donnée à ce réseau de réseaux.

L'architecture Internet se fonde sur une idée simple : demander à tous les réseaux qui veulent en faire partie de transporter un type unique de paquet, d'un format déterminé par le protocole IP. De plus, ce paquet IP doit transporter une adresse définie avec suffisamment de généralité pour pouvoir identifier chacun des ordinateurs et des terminaux dispersés à travers le monde. Cette architecture est illustrée à la figure suivante.

Nous allons traiter dans cette partie les protocoles, fonctionnalités et applications d'internet

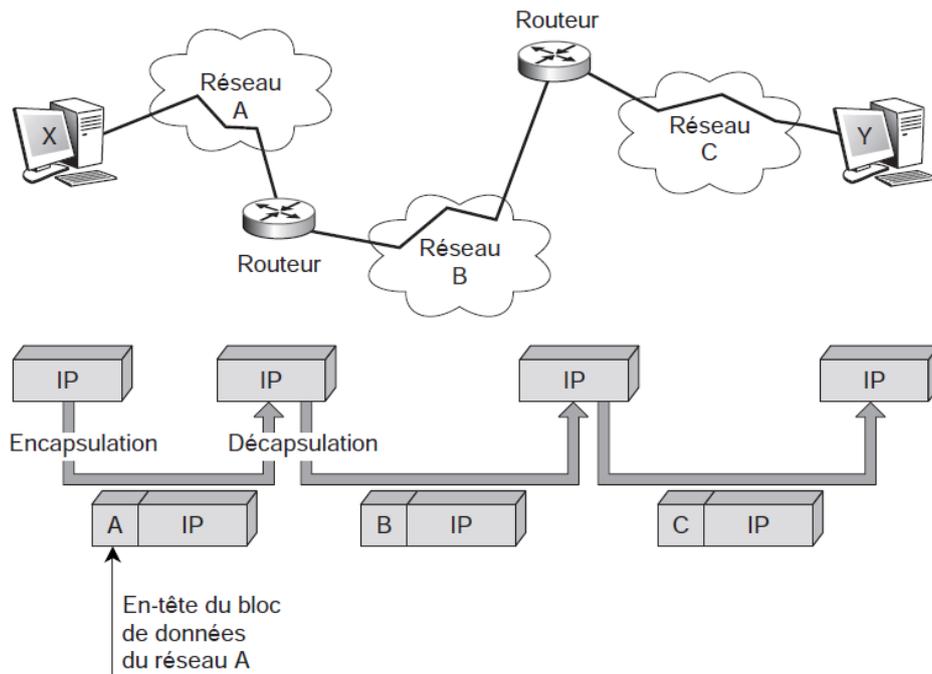


Figure 8. Architecture d'internet

### 3.1. Les générations du réseau internet :

On distingue deux catégories de réseaux Internet, l'Internet 1, qui est l'Internet actuel, et l'Internet 2, longtemps appelé IPng (IP Next Generation). Les sections qui suivent rappellent les caractéristiques de la première génération avant d'aborder la seconde. Quelques applications Internet classiques sont ensuite examinées, ainsi que des extensions débouchant sur de nouvelles applications.

- **Internet1** : Internet s'est rapidement développé pour interconnecter des milliers de réseaux aux États-Unis et en Europe. Au départ, il permettait de relier 20 000 ordinateurs dans les universités et les laboratoires de recherche. Alors que ses prévisions de croissance étaient de 15 % par an en 1987, aujourd'hui le réseau Internet croît à un rythme annuel de 60 %.
- **Internet2** : Lancé dans les années 95, le concept de l'Internet 2 vise à réaliser des réseaux dans lesquels une qualité de service puisse être délivrée aux utilisateurs. Plusieurs réseaux peuvent prétendre appartenir à cette nouvelle génération. Comme expliqué précédemment, l'introduction de cette nouvelle génération s'appuie en premier lieu sur une augmentation très importante des débits de façon à prendre en compte les applications multimédias.

### 3.2. Fonctionnement du réseau :

Pour les différents services Internet comme World Wide Web, Gopher, courriel, FTP.etc. Un logiciel serveur approprié doit être installé sur un ordinateur hôte qui propose des services à d'autres ordinateurs. Un hôte ne peut fournir un service Internet que si un logiciel serveur

approprié est actifs et si l'ordinateur est en ligne, et qu'aucun logiciel de protection (pare feu) n'empêche ou ne restreint les accès venant de l'extérieur [10]

### 3.2.1. Le serveur

Un serveur est un ordinateur ou un programme (logiciel) qui attend en permanence qu'une demande arrive concernant ses services. Ainsi par exemple un serveur www attend-il des demandes d'appel de pages HTML qui y sont sauvegardées.

### 3.2.2. Le client

Le client est un programme logiciel aussi qui réclame des données du serveur. Le navigateur web par exemple est un client. Pourtant, il y a aussi des « exceptions », ainsi un client ne peut-il pas seulement réclamer des données, mais aussi en envoyer au serveur.

### 3.2.3. L'architecture client/serveur

Le World Wide Web fonctionne suivant un modèle classique en informatique de gestion : client-serveur.

Deux acteurs sont mis en jeu : d'un côté le client qui effectue des requêtes en direction du serveur, de l'autre le serveur qui exécute ces requêtes et renvoie le résultat au client.

Client et serveur désignent non pas 2 personnes mais en réalité deux logiciels différents communiquant au moyen d'un système de règles ou protocole à travers un réseau (local ou étendu).

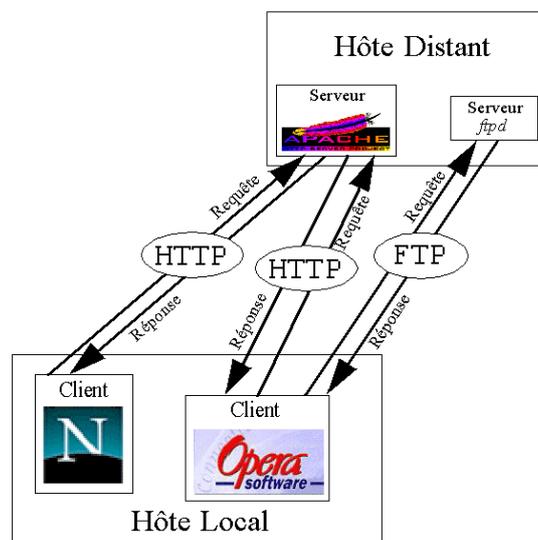


Figure 9. Modèle client/serveur.

Comme expliqué auparavant, un client lance des requêtes et le serveur renvoi des réponses suite aux demandes du client.

Clients et serveurs dialoguent de la façon suivante :

1. l'utilisateur à travers l'interface graphique de son navigateur, le logiciel client, exprime symboliquement une requête à l'adresse du serveur (par un clic de souris sur un *hyperlien* ou sur un bouton *submit* d'un formulaire ...)

2. le client traduit la demande conformément au protocole invoqué dans la requête (le plus souvent HTTP); voir services et protocoles, puis attend la réponse du serveur.
3. le serveur traite les données si nécessaire et retourne le résultat, le plus souvent le document demandé avec les fichiers annexés (images, sons ...)
4. le navigateur client met en forme cette réponse et la présente de façon convenable, compte-tenu des ressources de la station.

Lorsque la liaison physique est établie, les ordinateurs ainsi connectés doivent parler le même langage pour communiquer entre eux. [11]

### **3.3. Présentation du modèle TCP/IP**

#### *3.3.1. Description du modèle*

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le modèle TCP/IP, comme nous le verrons plus bas, s'est progressivement imposé comme modèle de référence en lieu et place du modèle OSI. Cela tient tout simplement à son histoire. En effet, contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation ; la normalisation est venue ensuite. Cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients.

L'origine de TCP/IP remonte au réseau ARPANET. ARPANET est un réseau de télécommunication conçu par l'ARPA (Advanced Research Projects Agency), l'agence de recherche du ministère américain de la défense (le DOD : Department of Defense). Outre la possibilité de connecter des réseaux hétérogènes, ce réseau devait résister à une éventuelle guerre nucléaire, contrairement au réseau téléphonique habituellement utilisé pour les télécommunications mais considéré trop vulnérable. Il a alors été convenu qu'ARPANET utiliserait la technologie de commutation par paquet (mode datagramme), une technologie émergente attrayante. C'est donc dans cet objectif et ce choix technique que les protocoles TCP et IP furent inventés en 1974. L'ARPA signa alors plusieurs contrats avec les constructeurs (BBN principalement) et l'université de Berkeley qui développait un Unix pour imposer ce standard, ce qui fut fait.

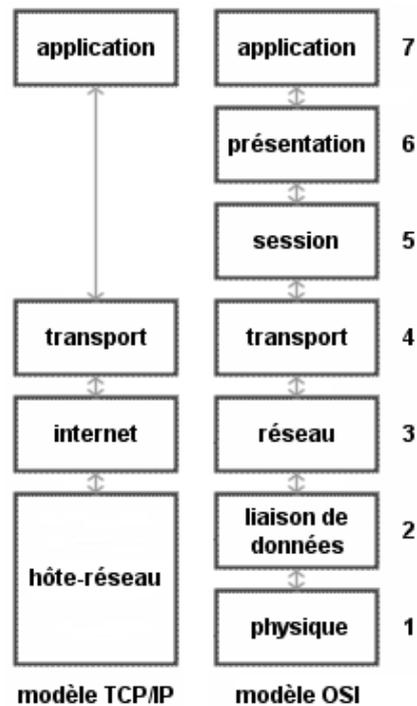


Figure 10. Comparaison entre le modèle OSI et TCP/IP

### 3.3.2. La couche hôte réseau

Cette couche est assez "étrange". En effet, elle semble "regrouper" la couche physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

### 3.3.3. La couche internet

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le roulage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol).

### 3.3.4. *La couche transport*

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation. Officiellement, cette couche ne peut utiliser que deux protocoles, soit TCP ou UDP.

### 3.3.5. *La couche application*

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs. [12]

## 3.4. **Les protocoles du réseau Internet**

### **Le protocole IP :**

Le protocole IP (Internet Protocol, RFC 791) est au cœur du fonctionnement d'un internet. Il assure sans connexion un service non fiable de délivrance de datagrammes IP. Le service est non fiable car il n'existe aucune garantie pour que les datagrammes IP arrivent à destination ; certains peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre. Le mode de transmission est non connecté car IP traite chaque datagramme indépendamment de ceux qui le précèdent et le suivant.

Le rôle du protocole IP est centré autour des trois fonctionnalités suivantes :

- Définir le format du datagramme IP qui est l'unité de base des données circulant sur Internet.
- Définir le routage dans internet.
- Définir la gestion de la remise non fiable des datagrammes.

## **Protocole TCP :**

TCP est un protocole de transport (couche3) orienté connexion. Il permet de fournir un flux d'octet fiable assurant l'arrivée des données sans altérations et dans le bon ordre, avec retransmission de paquets.

## **Le protocole UDP :**

Le protocole UDP utilise IP pour acheminer, d'un ordinateur à un autre, en mode non fiable des datagrammes qui lui est transmis par une application. UDP n'utilise pas d'accusé de réception et ne peut donc pas garantir que les données ont bien été reçues. Il ne réordonne pas les messages si ceux-ci n'arrivent pas dans l'ordre dans lequel ils ont été émis et il n'assure pas non plus le contrôle de flux.

Cependant, UDP fournit un service supplémentaire par rapport à IP, il permet de distinguer plusieurs applications destinataires sur la même machine par l'intermédiaire des ports. Un port est une destination abstraite sur une machine identifié par un numéro qui sert d'interface à l'application pour recevoir et émettre des données.

Chaque datagramme émis par UDP est encapsulé dans un datagramme IP en fixant à 17 la valeur du protocole.

### **3.5. Les applications Internet**

Les applications les plus classiques d'Internet comprennent la messagerie électronique SMTP, le transfert de fichiers FTP, le terminal virtuel Telnet, l'accès aux pages de fichiers distribués NFS et les applications liées au Web.

#### **SMTP (Simple Mail Transfer Protocol)**

SMTP a été l'une des premières applications Internet. Il définit une messagerie électronique relativement simple, qui se sert des adresses Internet, de type baghdad16@hotmail.com, où la deuxième partie représente le nom du domaine qui gère le serveur de messagerie.

Depuis 1993, un nouveau protocole de contenu a été défini avec le protocole MIME (Multipurpose Internet Mail Extensions), qui permet d'introduire dans le message des formats multimédias (vidéo, images, son...).

#### **FTP (File Transfer Protocol)**

FTP est un protocole de transfert de fichiers, qui permet de garantir une qualité de service. Le transfert s'effectue entre deux adresses extrémité du réseau Internet. L'application FTP est de type client-serveur, avec un utilisateur, ou client, FTP et un serveur FTP.

#### **Telnet**

Telnet est une application de connexion à distance, qui permet de connecter un terminal à une machine distante. C'est l'application de terminal virtuel.

#### **Usenet News**

Les Usenet News correspondent à des forums d'utilisateurs ayant en commun un sujet de discussion. Chaque utilisateur du groupe peut ajouter ses propres documents sous forme de fichiers. Le forum possède une liste d'utilisateurs, lesquels sont libres de supprimer leur nom ou de l'ajouter lorsqu'ils le veulent. Il n'existe aucun administrateur pour ces services. Les

bornes à ne pas franchir correspondent à des règles de bonne conduite, définies dans une « netiquette », sans grande précision toutefois.

Le protocole NNTP (Network News Transfer Protocol) a été développé pour permettre aux utilisateurs d'accéder aux serveurs Usenet et de discuter entre eux.

### **Gopher**

Gopher est un système de fichiers répartis sur des serveurs distribués, accessibles par le biais de menus communs à l'ensemble des serveurs.

### **WWW (World-Wide Web)**

Le World-Wide Web est un système de documents hypermédias distribués, créé par le CERN (Conseil européen pour la recherche nucléaire) en 1989. Ce système travaille en mode client-serveur et utilise les logiciels navigateurs tels que Google chrome, Netscape ou Microsoft Internet Explorer pour permettre à l'utilisateur de naviguer dans le système de bases de données distribuées.

Les clients et les serveurs du Web utilisent le protocole de communication HTTP (HyperText Transfer Protocol). Le langage sous-jacent, HTML (HyperText Markup Language), permet de définir une utilisation spécifique du document. Les liens hypertextes indiqués par des zones de texte permettent de relier les documents entre eux, quelle que soit la localisation géographique de ces documents. L'ensemble de ces liens entre documents forme la toile d'araignée, ou Web, sur laquelle il est possible de naviguer.

### **Les applications Peer-to-Peer**

Les applications Peer-to-Peer, aussi appelées P2P, font partie du panorama d'Internet depuis le début des années 2000, et des pointes de plus de 50 p. 100 du trafic Internet global ont été observées. Ces applications, qui ont été popularisées par Napster, torrent, e-mule... correspondent à des trafics allant directement de machines terminales à machines terminales.

## **4. Internet mobile**

À partir des années 2011, 2012, les applications dans l'environnement mobile seront les mêmes que dans les environnements fixes. L'augmentation des débits procurée par les réseaux UMTS et Wi-Fi est telle que données, parole et vidéo se superposeront, même si la qualité de la parole ou de l'image restera inférieure à l'équivalent en réseau fixe.

Pour le moment, et dans beaucoup de pays émergents les applications pour réseaux de mobiles sont assez différentes de celles que l'on trouve dans les réseaux fixes du fait des très faibles débits disponibles sur les interfaces hertziennes en comparaison des vitesses d'accès aux réseaux filaires. De plus, il faut différencier les applications pour les réseaux sans fil et les réseaux de mobiles étant donné les fortes différences de débit aujourd'hui.

Dans les pays développés, le débit dans les réseaux sans fil, s'approche des valeurs atteintes dans le fixe, ce qui induit un développement rapide du multimédia sur ce type de réseau. Les protocoles utilisés ne sont d'ailleurs pas différents des principaux protocoles déjà présentés au préalable. En revanche, les débits des interfaces des réseaux de mobiles restent

d'un ordre de grandeur faible comparé aux autres réseaux, allant de 9,6 Kbit/s pour le GSM à quelque 30 Kbit/s pour le GPRS et peut-être 50 Kbit/s en moyenne pour l'UMTS. Le cas de l'UMTS pose cependant de nombreux problèmes, car si l'on peut s'attendre à des débits relativement importants en période creuse, de 384 Kbit/s à 10 Mbit/s, ils ne devraient pas dépasser 50 Kbit/s en moyenne dans les périodes chargées.

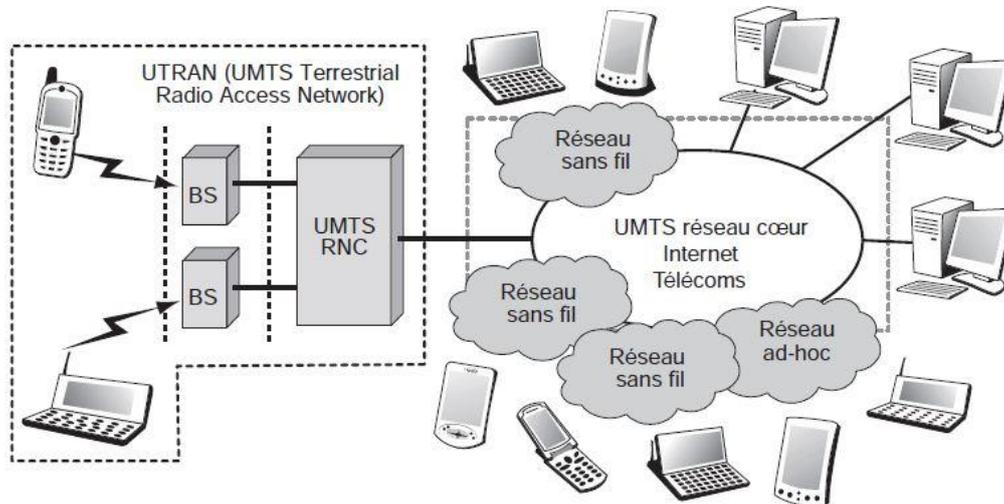


Figure 11. Environnement de l'Internet mobile

#### 4.1. Les applications de l'internet mobile

Les applications de l'Internet mobile regroupent de nombreux services, comme le WAP, i-Mode, les services de radiomessagerie de type pager, les applications à base de HTML allégé, les jeux distribués, la télévision interactive, ainsi que des services liés à la parole. Ces applications ont en commun de ne gérer aucune persistance de l'information sur le terminal mobile connecté, tout se passant sur un serveur d'applications.

La puissance des nouveaux terminaux mobiles virtuels, comme les PDA, change fondamentalement les choses. Ces terminaux se comportent comme des ordinateurs standards, et les applications y sont traitées comme sur une machine terminale fixe. En conséquence, des protocoles tels que le WAP deviennent totalement inutiles, puisqu'il suffit d'utiliser directement HTTP.

Les applications de base de l'Internet mobile sont de type client-serveur, le terminal ne servant que d'affichage. Le débit des communications est très faible.

##### 4.1.1. Le WAP (Wireless Application Protocol)

Le WAP utilise un langage particulier dérivant du XML, appelé WML (Wireless Markup Language), ainsi qu'un langage de script, WMLScript, qui autorise la transmission de pages Internet sur des téléphones portables.

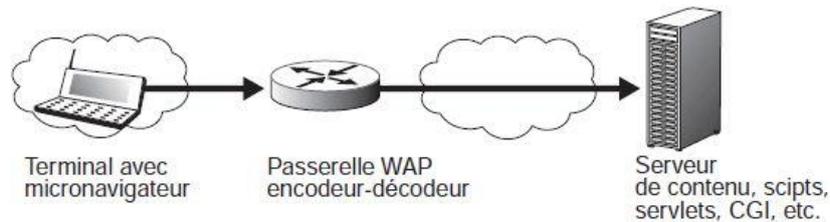


Figure 12. Communication WAP

Les terminaux peuvent être des téléphones WAP, des PDA, des Handheld PC, etc. Ils possèdent un micro navigateur, qui est soit chargé par l'utilisateur, soit fourni avec le terminal. Ce micro navigateur est généralement dépendant de l'équipementier, (Opera mini, Safari, Deep Fish,

Voici l'architecture protocolaire WAP :

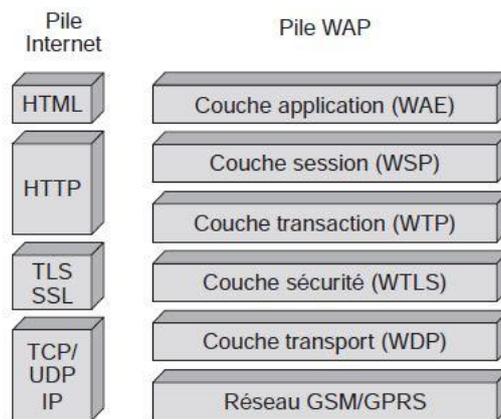


Figure 13. Architecture protocolaire WAP

#### 4.1.2. Le I-mode

Le standard japonais i-Mode, de NTT DoCoMo, utilise du C-HTML (Compact HTML), c'est-à-dire du HTML sans cadre, animation Flash ni JavaScript.

Le C-HTML est un sous-ensemble du HTML destiné à fonctionner sur des navigateurs mobiles allégés. Il est en cela comparable au format utilisé sur certains navigateurs Internet équipant les assistants personnels de type Pocket PC. L'ergonomie globale des téléphones i-Mode reste cependant assez proche de celle des téléphones GSM ou GPRS, avec un écran certes de petite taille, mais en couleurs.

Comme le langage utilisé par i-Mode est dérivé du HTML, il ne nécessite pas d'étape intermédiaire de conversion en binaire, à l'inverse du WAP, qui réclame l'emploi d'une passerelle. L'accès aux pages se fait en direct, comme pour les assistants personnels, *via* les couches réseau. Grâce à la technique i-Mode, qui permet d'afficher rapidement une page sur l'écran couleur, et à une stratégie marketing bien ciblée vers les jeunes, NTT DoCoMo est devenu le premier opérateur de mobiles à réaliser des bénéfices sur un système équivalent au WAP. Au Japon, le trafic de l'Internet mobile est à présent supérieur au trafic généré par la voix téléphonique grâce à cette application i-Mode.

## 5. La passerelle WAP

La passerelle WAP est l'élément qui différencie le WAP du Web. Elle assure deux fonctionnalités principales :

Elle réalise la connexion entre le réseau informatique et le réseau téléphonique sans fil, elle code et décode les requêtes et les réponses entre le terminal mobile et le serveur Web.

Elle peut être hébergée soit chez un opérateur mobile, soit chez un fournisseur d'accès, soit resté en interne au sein de l'entreprise. L'intérêt de la dernière solution réside dans le fait que l'entreprise garde ainsi la maîtrise des connexions WAP. [13]

### 5.1. Fonctionnalités de la Gateway WAP

Nombreuses sont les fonctions d'une Gateway WAP, mais elles ne sont pas obligatoirement toutes implémentées. La liste ci-dessous nous en donne un premier aperçu :

- Implémentation du protocole à couches WAP
- Contrôle d'accès.
- Protocole de conversion WAP en http.
- Conversion HTML en WML.
- Encodage du WML.
- Compilation du WML Script.
- Sécurité.

## 6. Les serveurs

Nous allons présenter quelle que serveurs que nous aurons besoin par la suite :

### 6.1. Serveur web :

Un serveur WEB est un ordinateur sur lequel fonctionne un logiciel serveur http, mais peut être aussi désigné le serveur HTTP (le logiciel) lui-même. Les deux termes sont utilisés pour le logiciel car le protocole HTTP a été développé pour le Web et les pages Web sont en pratique toujours servies avec ce protocole.

La plupart des ordinateurs utilisés comme Serveur Web sont reliés à internet et hébergent des sites Web.

Les serveurs Web les plus utilisés sont :

- Apache HTTP Server de Apache Software Foundation, successeur du NCSA ;
- Internet Information Services de Microsoft ;
- Sun Java System Web Server de Sun Microsystems (anciennement iPlanet de Netscape Communications Corporation, puis Sun One de Sun Microsystems) ;
- Le serveur Web Zeus de Zeus Technology.

## 6.2. Serveur de base de données

Un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs bases de données. Il s'agit typiquement de demandes de recherche, de tri, d'ajout, de modification ou de suppression de données.

Le serveur de base de données fait partie d'un système de gestion de base de données (abréviation SGBD) qui comporte un logiciel client et un logiciel serveur. Les demandes de manipulation de données sont souvent créées par un logiciel de gestion sous forme de requêtes en langage SQL, puis le client les transmet au serveur en utilisant un protocole propre au SGBD.

Une application informatique en architecture trois tiers comporte typiquement un serveur de base de données (tiers 3) avec un serveur web (tiers 2) et un navigateur web (tiers 1). L'application hébergée par le serveur web est le client du serveur de base de données.

L'un des SGBD les plus connus sont : Oracle, Microsoft SQL Server ou MySQL

## 6.3. Serveur dédié

Un serveur dédié est un serveur qui est mis à disposition d'un seul client par un hébergeur. Le serveur dédié peut être administré à distance via le réseau Internet ou administré par l'hébergeur. Dans le second cas, on parle de serveur dédié info géré.

On parle de machine entièrement dédiée par un hébergeur de sites Web lorsque le client a la possibilité de gérer, non seulement les fichiers sur le serveur, mais également les applications ainsi que leurs configurations et de serveur semi-dédié lorsque le client a uniquement accès aux fichiers du serveur.

## 7. Conclusion

Ce chapitre représente les différents réseaux mobile cellulaire comme hertziens, ainsi qu'un aperçu sur l'internet et son développement fixe et mobile ainsi que son développement ainsi que ces différentes applications et domaine d'utilisation.

Par la suite nous avons présenté les différents outils et protocoles d'accès que nous aurons besoin par la suite dans la réalisation de notre solution.

# C

## hapitre 2 :

### E-business & technique de sécurité

« Dans la vie rien n'est à craindre, tout est à comprendre ». Marie Curie

## Introduction :

Ils sont plusieurs millions de personnes à se connecter tous les jours à internet, cette dernière qui est devenu un moyen très efficace pour pratiquer du commerce et ainsi on peut acheter et vendre par le biais du net. Un commerçant professionnel est amené dans la plupart des cas à commercialiser plusieurs types de produits et de services, il devra donc penser à gérer tout ça en impliquant plusieurs utilisateurs. Ces utilisateurs seront amenés à leur tour à exécuter plusieurs tâches commerciales et même administratives dont par exemple : établissement d'une facture pour le client. Les problèmes rencontrés dans ce genre de systèmes sont les suivants :

- une plate forme quasi inexistante pour le E-commerce ainsi qu'avec une population majoritairement non bancarisé et le retard enregistré pour le paiement électronique.
- Inefficacité de la stratégie de commercialisation des produits / services.
- Lourdeur des différentes gestions (commandes, clients, stock), ce qui ne permet pas d'avoir une bonne synchronisation entre les commandes passées avec le stock disponible et donc un retardement des processus de livraison et paiement.

Nous allons donc débiter ce chapitre avec des définitions et du texte théorique dans le but de se familiariser avec les deux concepts abordés au cours du projet et qui sont : l'E-commerce et l'E-paiement.

On va définir l'E-commerce et ses fonctions puis décrire le fonctionnement de ses différents processus. Il est aussi important de citer les raisons qui peuvent pousser un marchand vers le commerce électronique.

Pour le paiement électronique, nous allons définir ce concept ainsi que son fonctionnement pour pouvoir le relier au commerce électronique. Une fois la liaison faite, on peut décrire comment le paiement classique peut s'adapter sur le web selon les moyens existants.

## Le E-business :

Le E-business (Electronic business) parfois traduit en affaires électroniques, correspondent à une notion très vaste que l'on pourrait synthétiser par l'utilisation de moyens électroniques (particulièrement des techniques de l'information et de la communication) pour réaliser des affaires (business en anglais). Ce sont souvent les techniques de l'internet et le Web qui viennent à l'esprit, mais en fait presque toutes les techniques informatiques et de télécommunications interviennent dans le domaine des affaires électroniques. Les affaires électroniques existaient d'ailleurs bien avant l'apparition de la Toile, même si celle-ci a permis une meilleure visibilité de ce domaine par le grand public.

Les méthodes proposées par les affaires électroniques permettent aux entreprises de mettre en œuvre leurs processus plus efficacement et avec plus de souplesse tant en interne qu'avec les entités extérieures. Ces méthodes permettent de travailler plus étroitement avec les fournisseurs et partenaires, dans le but de satisfaire au mieux les besoins et les attentes des clients.

En pratique, l'utilisation du commerce électronique conduit à de nouvelles sources de revenu, à l'amélioration des relations avec les clients et partenaires, et à une meilleure efficacité par l'emploi des systèmes de gestion des connaissances. Les affaires électroniques peuvent se déployer à travers le réseau Internet public, des réseaux internes (Intranet) ou externes (Extranet) privés et sécurisés, ou plus généralement tout moyen de communication électronique.

L'E-business ne se réduit pas au commerce électronique. Il couvre également tous les processus impliqués dans la chaîne de valeur : les achats électroniques (E-procurement en anglais), la gestion de la chaîne d'approvisionnement avec le traitement électronique des ordres, le service à la clientèle, et les relations avec les partenaires ainsi le paiement électronique . Cela s'applique aux organisations traditionnelles et virtuelles. Les standards techniques propres à l'E-business facilitent les échanges de données entre les entreprises. Les solutions logicielles intégrant ces standards permettent l'intégration des processus au sein des entreprises mais aussi entre les entreprises.

## **I. Partie I : le commerce électronique :**

### **1. Commerce électronique**

« L'ensemble des échanges numérisés liés à des activités commerciales qui prendrais en considération : Personnes & organisme, Produits, Mode de transmission ». (*Francis Lorenz*)

#### **1.1 Introduction**

« Aujourd'hui, la plupart des entreprises du commerce en détails s'adaptent progressivement au commerce électronique via l'internet. Pour les grandes entreprises de la vente à distance, le réseau informatique complète le courrier et le mobile. Il leur permet une relation plus interactive avec le client. Personnaliser cette relation est aussi une motivation pour les entreprises traditionnelles du commerce en magasin, qui misent sur l'image favorable du web auprès des consommateurs. Le commerce en ligne est également le fait de petites entreprises créées spécifiquement pour exercer cette activité. Les détaillants attendent du commerce électronique une augmentation de la clientèle et du chiffre d'affaire mais craignent une augmentation de la concurrence. » [15]

Nous allons voir dans cette partie un historique et des généralités sur l'E-commerce ; nous y concentrons notre étude sur le modèle « B to C » car c'est le modèle sur lequel se base notre système.

Nous allons donc voir les possibles stratégies adoptées du « B to C », et recenser différents avantages et inconvénients pour les deux parties du modèle « B to C ».

#### **1.2 Historique**

« Les débuts et l'évolution du E-commerce sont liés avec l'évolution d'Internet. Depuis quelques années, le secteur de l'Internet enregistre des chiffres de croissance impressionnants.

Au tout début, Il y'avait un manque d'autorité capable de définir des règles et des sanctions ce qui a laissé apparaître une certaine forme d'anarchie sur Internet et a largement freiné le développement d'activités commerciales sur ce réseau. Il y avait également d'autres facteurs expliquant le retard de l'arrivée du E-commerce, prenant comme exemple, la langue principale dans les débuts de l'Internet, était l'anglais, l'ergonomie et le graphisme étaient très poussés mais aussi, l'esprit des principaux acteurs d'Internet, dans les années 80 et 90 étaient orientés vers le partage gratuit et libre de l'information. Esprit, là encore, peu compatible avec des activités commerciales. » [16].

« Depuis l'ouverture du réseau au grand public et la généralisation des accès à Internet ont complètement contrecarré ces facteurs de ralentissement. Même si l'esprit de gratuité de l'information est toujours présent, ce changement devait se faire. Le réseau ne pouvait continuer à accueillir un nombre d'utilisateurs toujours plus nombreux sans mettre en place un modèle économique viable. Vu Le coût des équipements et infrastructures de télécommunication ne pouvait être financé que par les seuls abonnements versés aux fournisseurs d'accès à Internet. » [17].

« Le lancement des activités commerciales sur Internet est apparu dans les années 90, et Il n'en demeure pas moins que le commerce interentreprises qui a constitué en l'an 2000 plus de 80% des échanges commerciaux électroniques. Au total il a été estimé que le chiffre d'affaire du commerce électronique représente la somme de 40 Milliards de dollars en 2000 selon une étude de l'époque. La naissance et le développement de l'E-commerce sont liés à des évolutions technologiques du réseau Internet, en générale le développement de la vente à distance à l'évolution même de la couverture de ce réseau sur la société. » [18].

### **1.3 Généralités sur l'E-commerce**

Nous allons voir quelques définitions et généralités sur l'E-commerce :

#### **1.3.1 Qu'est ce que le E-Commerce?**

« Selon la définition de l'encyclopédie, On appelle « Commerce électronique » (ou E- Commerce ou le E-business) l'utilisation d'un média électronique pour la réalisation de transactions commerciales et l'échange de biens et de services entre deux entités sur les réseaux informatiques. La plupart du temps il s'agit de la vente de produits à travers le réseau internet, mais le terme de E-Commerce englobe aussi le commerce interentreprises ou l'on utilise des réseaux de type E.D.I (Échange de données informatisées). Il y'a aussi des transactions électroniques sur les réseaux téléphoniques qu'on appelle le « M-commerce » (mobile commerce) » [19].

#### **1.3.2 Pourquoi E-Commerce ?**

« Grâce à sa flexibilité, sa large diffusion et au fait qu'une boutique en ligne est ouverte 24h/24 tous les jours de l'année, le commerce électronique devient chaque jour un outil de vente plus important aux yeux des entreprises modernes. Même les entreprises les plus traditionnelles exploitent désormais Internet afin de stimuler leurs ventes et se lancent dans l'aventure du commerce électronique.

Au fil des nouvelles technologies, les sites de ventes en ligne possèdent des systèmes de paiements de plus en plus sécurisés. Les sites e-commerces étant de plus en plus contraints à une plus grande transparence quant à la non diffusion des informations personnelles de leurs clients. Les lignes hautes débit se sont démocratisées, et il est maintenant possible de recevoir un certain trafic à moindre coût. Grâce aux médias présents sur internet, les internautes sont mieux informés du risque totalement inexistant de commander des produits en ligne, et encore bien d'autres raisons...

Le prix est plus attractif sur Internet car les frais de fonctionnement sont moindres, (pas d'employé pour votre showroom, etc...). La comparaison des prix de chacun des marchands peut se faire très rapidement par le biais de comparateurs de prix. Les délais de livraison proposés sont très courts (48 heures au max). Les produits peuvent désormais être réservés avant leur date de commercialisation officielle, etc. » [20].

#### 1.4 Déroulement et Processus impliqués dans l'E-commerce :

Le E-Commerce, et dans une plus large mesure le E-business, via une multitude de plate-forme :

- un site web.
- téléphone mobile avec un site internet version mobile.
- une application mobile.
- par SMS.
- Un serveur vocal interactif ACD.

Le E-commerce implique un grand nombre de processus : de la navigation à la commande, gestion de la commande à l'envoi du produit, du service après-vente au traitement des avis des clients, toutes ces étapes sont cruciales pour une société d'E-Commerce.

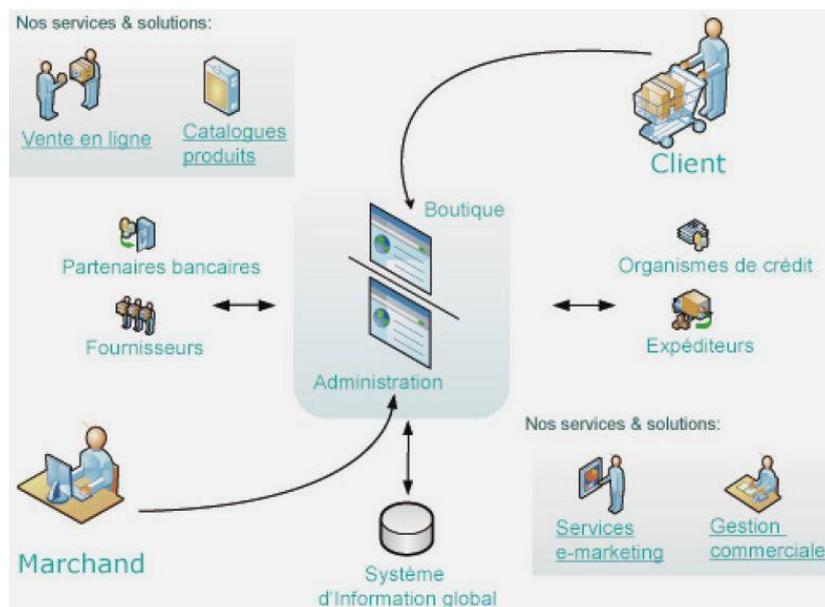


Figure 14. Les différents composants de l'E-commerce [21].

« Pour qu'un client accède à un site de vente en ligne il faut d'abord qu'il le trouve : le référencement est si important qu'il est même devenu le nouveau nerf de la guerre sur internet. Une fois sur le site, le client devra à la fois trouver le site agréable et fonctionnel : s'il ne trouve pas ce qu'il cherche en quelques clics, le client ira ailleurs.

Sinon avec une stratégie de conquête clients : avec une publicité ciblée via les réseaux sociaux comme FACEBOOK, TWITTER, YOUTUBE, VIADEO, MY SPACE, et des spots publicitaires sur le différent support de media.

Avec les nouvelles technologies, le client est alerté pour toutes les promotions qui lui intéressent en permanence, où en est sa commande : l'étape de la logistique est l'une des plus déterminantes de l'opinion du client...

Donc il faut que le client soit pris en considération, avoir le sentiment qu'on pense à lui, que notre site est fait suivant ses attentes, et cela dès la première étape de conquête clients jusqu'à la vente d'un produit et le suivi qui va avec.

Toutes ces étapes résument parfaitement la philosophie d'une solution e-Commerce prendre en compte tous les processus pour pouvoir booster un chiffre d'affaires.

Donc les transactions de commerce électronique se déroulent généralement comme suit : un acheteur consulte un catalogue en ligne, commande un article ou un service et fournit ses informations de carte de crédit ainsi qu'une adresse de livraison. Le vendeur vérifie ensuite les informations du moyen de paiement, traite la commande et s'occupe de la livraison. » [22].

### **1.5 Fonctions de l'E-commerce :**

Les principales fonctions de l'E-commerce sont :

- ❖ Inscription et validation des clients et utilisateurs (gestion des profils)
- ❖ Obtention d'un devis.
- ❖ Conseil et catalogue électronique.
- ❖ Gestion du panier, commandes et achat en ligne.
- ❖ Gestion des stocks en temps réel (tableau de bord).
- ❖ Paiement en ligne.
- ❖ Suivi de la livraison.
- ❖ Service après vente en ligne.

### **1.6 Type d'échange B2C**

Le commerce électronique B to C, autrement dit, le commerce électronique grand public sur Internet est sans doute l'aspect le plus viable du commerce électronique car il permet au consommateur d'acheter directement sur Internet des biens et des services pour son usage personnel.

Dans ce type de commerce, l'entreprise peut utiliser un questionnaire on-line qui lui permettra de mieux connaître ses clients, d'individualiser les contrats, les offres et d'accompagner les prospects de la commande jusqu'à la livraison.

## 1.7 Stratégies dans le e-commerce du type B to C

On retrouve 5 stratégies qui permettent d'intégrer l'E-commerce à l'entreprise: [23].

### 1.7.1 *Clic & Mortar*

Ça veut dire « clic et mortier », c'est-à-dire Internet combiné au magasin traditionnel. Cette stratégie offre donc plusieurs possibilités aux clients : repérer le produit sur le net et l'acheter en magasin, repérer le produit en magasin et l'acheter sur le net, sur tous avec l'intégration de l'option de géo-localisation dans le site.

### 1.7.2 *La vitrine commerciale*

Il s'agit d'un site institutionnel (ou Corporate en anglais) présentant de manière statique les différents produits de l'entreprise. Sorte de catalogue online, ce type de site tend pourtant à disparaître, même si son principal avantage réside dans le fait que l'entreprise peut le concevoir elle-même.

### 1.7.3 *Boutique (ou site marchand)*

C'est un site commercial privé ayant pour objectif la vente de produits en e-commerce. C'est le plus compliqué à réaliser et suppose une solution de paiement en ligne et c'est cette stratégie que nous allons voir dans la conception et dans la réalisation.

### 1.7.4 *Galerie en ligne*

C'est un centre commercial virtuel dans lequel plusieurs entreprises non concurrentes se regroupent permettant ainsi au cyber-consommateur de trouver à la même adresse une offre élargie et complémentaire (livres, vêtements, électroménager...). Cette solution permet aux entreprises de réduire les frais d'accès au réseau et de bénéficier d'une importante zone de chalandise pour une somme raisonnable.

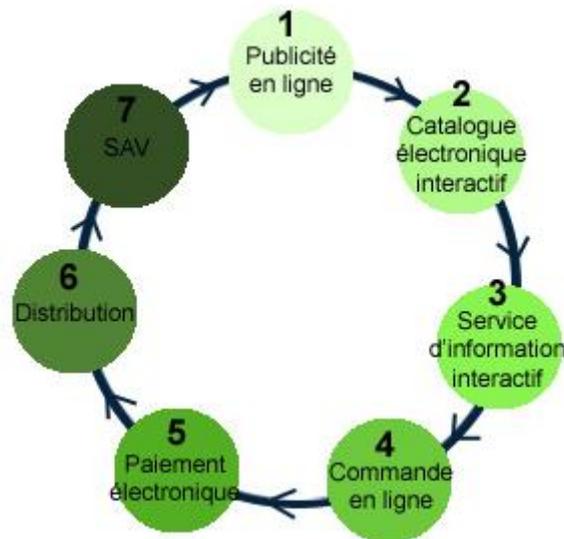


Figure 15. Les sept briques de l'E-commerce B to C [24].

Plus le vert est foncé, plus la brique est compliquée à mettre en place.

## 1.8 Avantages et inconvénients du e-commerce type B to C

Le commerce électronique sur Internet offre de nombreux avantages :

### 1.9 Les avantages

Les avantages sont classés selon deux parties : avantages pour la société et avantages pour les clients [25].

#### 1.9.1 Pour l'entreprise :

- ✓ Il ouvre un nouveau canal de distribution, un circuit complémentaire pour certains produits et services de l'entreprise.
- ✓ Il permet de couvrir des niches de marché dont l'atteinte serait jugée trop onéreuse par les moyens classiques de commercialisation.
- ✓ Il apporte une plus forte convivialité par rapport à la VPC (vente par correspondance) et à la commande à distance traditionnelle grâce aux multimédias qui regroupent le son, l'image, la couleur, le texte et l'animation.
- ✓ Il favorise l'interactivité en développant une relation personnelle avec le consommateur ou le client, facilitant la vente « one to one » (personnalisée).
- ✓ Il permet d'envisager des politiques de fidélisation du client à travers une offre de services et à forte valeur ajoutée.
- ✓ Il facilite les transactions en évitant à l'acheteur de se déplacer.
- ✓ Il donne la possibilité de réduire les prix publics des produits en éliminant la marge laissée habituellement aux intermédiaires.
- ✓ L'enregistrement des données via Internet est quasiment automatique et demande peu d'effort donc moins de personnel.

« Il recueille une masse précieuse d'informations sur les habitudes, les besoins de l'internaute. Ainsi, plus l'utilisateur visite le site, plus on apprend à le connaître par des séries de clics. En décortiquant les séances de clic (ou clic Stream), il devient alors possible d'établir des profils de consommateurs permettant d'adapter progressivement le e-marketing du site afin d'en retirer le maximum de profits. » [26].

### 1.9.2 Les facteurs d'incitation au E-commerce :

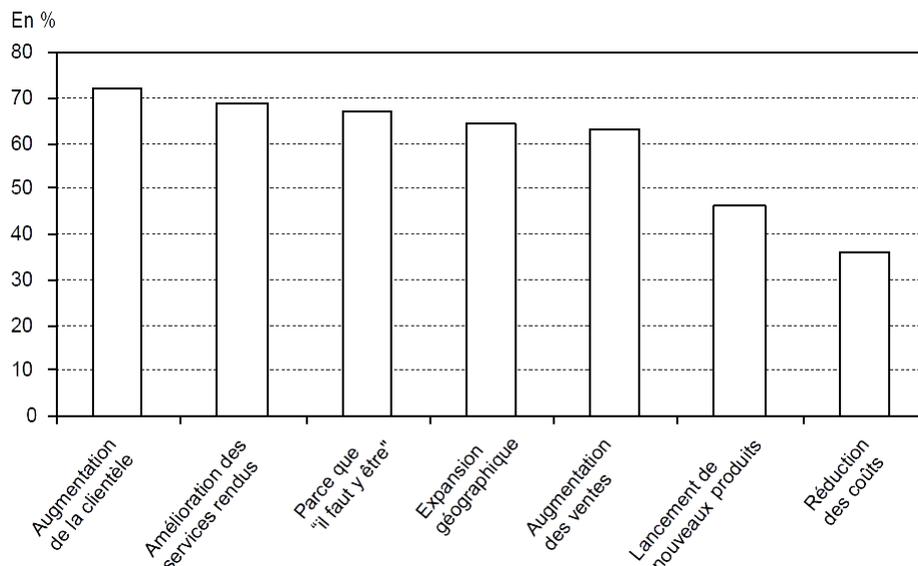


Figure 16. Les facteurs d'incitation à l'E-commerce. [27]

### 1.9.3 Pour les clients

Et pour les clients les avantages suivants :

- ✓ L'E-commerce est un excellent outil de présélection.
- ✓ La recherche du meilleur prix.
- ✓ Pas de pression de la part des vendeurs.
- ✓ Un marché de proximité à l'échelle mondiale.
- ✓ Il offre un gain de temps considérable.
- ✓ Une offre actualisée (mise à jour régulière).
- ✓ Connaître de nouveaux produits.
- ✓ Passer des commandes spécifiques.

### 1.10 Les inconvénients

Comme chaque outil commercial il présente aussi des inconvénients : [28].

### *1.10.1 Pour l'entreprise :*

- ✓ Les entreprises qui ont adopté ce mode rencontrent une résistance psychologique chez certains de ses clients.
- ✓ L'incertitude et le manque de confiance autour de la sécurisation des moyens de paiement, malgré le fait qu'actuellement les méthodes de cryptage de données assurent une confidentialité quasi parfaite lors de la transaction.
- ✓ La résistance des intermédiaires (grossistes, distributeurs) qui craignent une destruction d'emplois assortie d'une perte de chiffre d'affaire.

### *1.10.2 Pour les clients*

- ✓ Il permet le pistage informatique à partir des cookies, c'est-à-dire ces petits fichiers qui identifient l'ordinateur appelant de façon unique afin pouvoir retracer toutes les habitudes d'appel et de consommation.
- ✓ L'insécurité des paiements et la peur de tomber sur un cybermarchand mal honnête qui ne livre pas.
- ✓ Le manque de relations humaines et le sentiment d'isolement devant sa machine (cas des internautes peu expérimentés).
- ✓ Le manque de contact avec le produit.
- ✓ Les détails et tarifs de livraison.
- ✓ Les difficultés de recours en cas d'ennuis.
- ✓ Peut engendrer une dépendance.

## **2. E-commerce en Algérie**

Si on veut procéder par achat en ligne il faudra avoir une connexion à internet et pour l'instant certains critères indiquent que l'Algérie est en train de se brancher aux autoroutes de l'information. La vitesse de propagation d'Internet ne cesse d'augmenter mais très lentement. « Un algérien sur quatre est utilisateur d'internet, au total, l'Algérie compte huit millions d'internautes, ce chiffre englobe aussi bien 900 000 utilisateurs disposant de leurs propres connexions à internet. » [29].

Tout le monde est d'accord sur le niveau du « retard Algérien » en internet et surtout le commerce électronique, ce qui provoque l'existence d'un consensus sur les conséquences qu'aurait, à terme, un tel retard. Outre la marginalisation de l'Algérie dans les activités liées aux technologies de l'information un trop grand attentisme pénaliserait les entreprises algériennes. A commencer bien sûr par les entreprises commerciales.

### **2.1 Modèle actuel des échanges commerciaux**

Les échanges commerciaux en Algérie se font toujours d'une manière tout à fait traditionnelle, le consommateur ou le demandeur est toujours contraint à se déplacer jusqu'au lieu de commerce (de la vente) pour pouvoir faire une commande ou acheter une marchandise

et c'est le cas sur tous les niveaux commerciaux : grand public et interentreprises. Ce mode de transactions a souvent constitué un obstacle aux déroulements des transactions commerciales interentreprises (B to B). Ces freins sont généralement dus aux retards qui peuvent avoir lieu pendant le transport de la marchandise ou bien pour des raisons de factures non réglées ou d'une mauvaise gestion de stock.

## 2.2 Intérêt économique du passage au E-commerce en Algérie

- ✓ Faciliter l'accès des PME aux informations sur les marchés étrangers.
- ✓ Renforcer la capacité exportatrice des entreprises algériennes et d'intégrer le marché international.
- ✓ Baisse des coûts.
- ✓ Augmenter la concurrence.
- ✓ Diversification des produits et services offerts aux clients.
- ✓ Atteindre des besoins non satisfaits par la voie traditionnelle.
- ✓ L'adhésion à l'organisation mondiale du commerce (OMC).

## 2.3 Causes du retard de l'e-commerce en Algérie

### 2.3.1 *Systeme bancaire non compatible*

- ✓ Systeme miné par la corruption et la fraude.
- ✓ Systeme de paiement traditionnel.
- ✓ Retard dans la transmission.
- ✓ Insécurité des transactions.
- ✓ Manque de confiance (crainte à l'imposition).

### 2.3.2 *La réglementation et la législation*

L'Algérie n'a toujours pas légiféré dans le domaine d'Internet. Ce vide juridique se fait de plus en plus ressentir et peut causer des dommages d'ordre économique, juridique et social... Les règles concernent les transactions électroniques, propriétés intellectuelles et les mineurs.

Dans le contexte de ce mémoire nous avons fait une recherche fructueuse du « pourquoi » et nous avons été mis en contact avec le ministère de Poste et télécom afin de trouver une solution à cette problématique. Dans cette rencontre nous l'avons incité à combler ce vide juridique et il y'a eu une convention de partenariat entre le ministère du commerce et le MPTIC.

### 2.3.3 *Economie informelle*

« En Algérie, le secteur informel est très influant, mis à part, le secteur des hydrocarbures. En ce qui concerne le commerce, l'informel représente 60 % du marché

national, soit 1,8 millions de marchands clandestins contre 1,2 millions de commerçants régularisés » [30].

### **2.3.4 Habitudes des consommateurs**

Les habitudes du consommateur algérien constituent un sérieux obstacle au développement du commerce électronique. Elles sont caractérisées par :

- ❖ L'usage du commerce à proximité et l'habitude de fréquenter un magasin et faire confiance au gérant.
- ❖ Les traditions sociotechniques telles que : relation à la modernité, aisance et confiance dans l'argent numérique notamment, sont quasiment inexistantes.
- ❖ Le degré d'acceptation du risque vis-à-vis de la perte ou du vol de la carte de paiement électronique est très minime.

## **Conclusion**

Le passage au commerce électronique constitue un vrai moteur de relance pour l'économie algérienne aussi pour faciliter la vie quotidienne des gens. Son introduction devient de plus en plus nécessaire et urgente vu la situation commerciale hyper développée dans le monde et son implantation va permettre aux entreprises nationales de s'engager dans le marché internationale.

De notre part, nous allons essayer d'élaborer un système de commerce électronique sous forme de Boutique en ligne (site marchand promotionnel) afin de répondre aux besoins du type d'échanges « B to B » & « B to C ».

A présent, le projet est très réalisable vu l'augmentation du niveau des TIC d'année en année ainsi qu'avec le développement du nouveau système de paiement électronique qu'on va étudier dans le prochain chapitre.

## **II. Partie 2 : le E-paiement**

### **Introduction**

« Lorsque l'on veut vendre sur Internet, se pose le problème du paiement électronique sécurisé. Quelle que soit l'activité ou la taille de la société, qu'il s'agisse de biens physiques à livrer, de services ou de produits numériques délivrés en ligne... le moment du paiement en ligne est crucial. Une étude indiquait d'ailleurs il y a quelques temps que 67 % des internautes qui réalisaient leur shopping en ligne s'arrêtaient avant la fin de ce dernier, ceci pouvant être lié au manque de choix ou de confiance, mais aussi par la peur du paiement en ligne.

C'est pourquoi les solutions de paiement se sont largement diversifiées : en plus des solutions dites "classiques", on voit se développer de plus en plus de solutions "modernes" dans le sens où elles se servent des nouvelles technologies comme les GSM ou le Wifi ; ou alors elles s'adaptent à une demande bien particulière comme les problématiques de micro

paiement qui ont fait leur apparition avec les offres "premium" de nombreux sites, ce qui a poussé les prestataires bancaires et techniques à trouver de nouvelles solutions. »

« Renouveler son nom de domaine, acheter des fournitures de bureau, payer ses liens sponsorisés, acheter des billets de train ou d'avion pour ses voyages d'affaires... un chef d'entreprise a mille et une bonnes raisons de recourir au paiement en ligne. Comment choisir la bonne solution de paiement, connaître les dangers des transactions financières en ligne et les méthodes pour payer en toute sécurité : des informations indispensables pour optimiser ses achats. » [36].

## 1. Définitions

### 1.1 Définition du paiement électronique (E-paiement)

« Le paiement électronique est un moyen permettant d'effectuer des transactions commerciales pour l'échange de biens ou de services sur Internet. Actuellement, il est très bien implanté et utilisé par la majorité des personnes et entreprises ayant un commerce sur internet. » [36].

### 1.2 Définition du Terminal de Paiement Electronique

« Un terminal de paiement électronique (aussi appelé TPE) est un appareil électronique capable de lire les données d'une carte bancaire, d'enregistrer une transaction, et de communiquer avec un serveur d'authentification à distance. »



Figure 17. Terminal de Paiement Electronique

### 1.2.1 Fonctionnement

Un TPE peut lire une carte grâce à son lecteur de carte à puce ou par son lecteur de piste magnétique. Il a la possibilité de se connecter à un serveur d'authentification grâce à son modem. La carte lue peut-être une carte bancaire, un porte-monnaie électronique ou tout autre carte à puce ou une carte au format SIM contenue dans un téléphone mobile.

Les différentes plates formes de paiement sont développées à partir des spécifications techniques présentées dans le Manuel du Paiement Electronique (MPE) établi par le groupement des Cartes Bancaires (CIB).

Le TPE peut être chargé avec une liste des cartes opposées, il refusera alors toute carte se trouvant dans la liste.

## 2. E-commerce et E-paiement

« Le paiement électronique constitue l'un des principaux freins au développement du commerce en ligne. Aujourd'hui encore, le grand public perçoit généralement Internet comme un espace non sécurisé où les numéros de carte bancaire peuvent être facilement volés. Cette peur, facilement compréhensible, est pourtant en partie exagérée dans le sens où donner son numéro de carte sur le web n'est pas plus dangereux que de le donner par téléphone ou que de confier sa carte à un serveur au restaurant. Le risque est peut être plus présent après la transaction, si les numéros de cartes sont imprudemment stockés sur un serveur.

Cependant, selon une étude France Télécom datée de Janvier 2003, la carte bancaire qui effraye tant de e-consommateurs est paradoxalement le moyen de paiement le plus utilisé sur Internet, avec plus d'un achat sur deux réalisé (55%) grâce aux moyens bancaires classiques (CB, chèques, mandats...). Suivent ensuite les paiements via Kiosque (35%), puis 7% par service audiotel, et enfin 4% par refacturation de son FAI.

Parallèlement, une étude Forrester de Mai 2003 annonce que les modes de paiement privilégiés par les internautes (dans le cadre de règlements de contenus payants en ligne) sont la refacturation par son FAI (36%), loin devant la carte bancaire (11%) et la carte prépayée (10%). Autant dire que la demande ne correspond pas vraiment à l'offre, ou que les internautes sont sous-informés quant aux différents moyens de paiement qui existent en dehors de la traditionnelle carte bleue. » [34].

## 2.1 Adaptation du paiement au contexte électronique

Le paiement possède plusieurs modalités qui méritent une attention particulière au regard du commerce électronique. Le moment du paiement, son lieu, les frais qui y sont relatifs, ainsi que la quittance, sont autant d'éléments susceptibles d'y être modifiés. De la même façon, l'utilisation des moyens de paiement traditionnels tel que la carte de crédit, le chèque et l'argent comptant est différente lorsque les parties à la transaction ne sont pas en contact direct. Enfin, les moyens de preuve sur support électronique sont différents de ceux disponibles dans le cadre du commerce traditionnel.

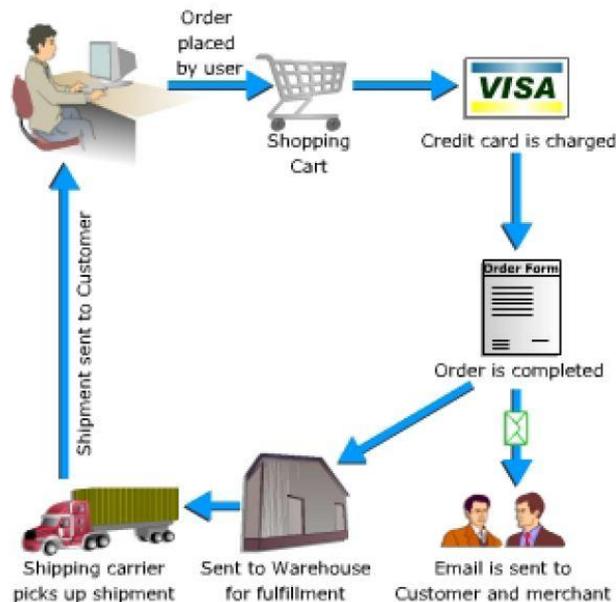


Figure 18. Schéma de déroulement d'un achat.

## 2.2 Moment du paiement

Le choix du moment où le paiement sera dû et laissé à la discrétion des parties. Celles-ci fixent le moment du paiement avant ou après l'exécution de l'obligation principale, en fonction de ce qui convient le mieux à leur situation particulière.

Dans la pratique du commerce électronique, le commerçant exige presque toujours le paiement au moment de l'envoi de la commande. Il s'agit d'une forme de paiement anticipé puisque celui-ci a lieu avant l'exécution de l'obligation.

## 2.3 Lieu du paiement

L'endroit où le paiement doit être effectué relève de la volonté des parties. Lorsqu'une transaction est conclue par le biais d'un site Web, les parties semblent convenir implicitement que le lieu du paiement se situe sur la plate-forme de paiement fournie à l'adresse du commerçant.

## 2.4 Quittance

La quittance est une attestation écrite par laquelle le commerçant libère le consommateur de son obligation envers lui. Une fois le paiement exécuté, le consommateur a droit à celle-ci. Dans le contexte des environnements dématérialisés, la quittance devrait prendre la forme d'un courrier électronique. Le simple affichage d'une page sur le site Web du commerçant ne semble pas suffisant puisque celle-ci peut s'avérer difficile à conserver pour le consommateur. Le courrier électronique devrait être envoyé automatiquement au moment du paiement afin de confirmer le bon déroulement de la transaction.

### **3. Moyens de paiement en ligne**

#### **3.1 Payer par carte bancaire**

« L'acheteur utilise sa carte bancaire classique pour payer. Il faut bien sûr vérifier que le site d'e-commerce sur lequel on fait nos achats est équipé d'un système de paiement sécurisé. C'est un mode de cryptage des données personnelles (nom, adresse, coordonnées bancaires) qui les rend invisibles et donc qui ne peuvent pas être récupérées par les hackers. Une fois certain de la sécurisation du site, le payeur communique ses coordonnées : Nom et coordonnées bancaires (16 chiffres + 4 chiffres de la date de validité + 3 chiffres du pictogramme au dos de la carte). » [37].

#### **3.2 Payer par E-numéro de carte**

C'est un moyen de paiement rattaché à la carte bancaire qui permet de payer sans donner son numéro de carte bancaire. Des E-numéros sont attribués, des numéros de carte bancaire temporaires.

#### **3.3 Payer sans carte bancaire**

Ce sont des services très appréciés par les internautes : ils permettent de régler ses achats sans communiquer son numéro de carte bancaire. Ils offrent aussi des tas de services connexes très intéressants pour un chef d'entreprise.

Le fameux service Paypal et son concurrent Google Checkout. Ces solutions de paiement en ligne nécessitent une adresse email et un numéro de carte bancaire (vous le communiquez uniquement à Paypal lors de l'inscription). Avec un compte Paypal, vous pouvez également recevoir de l'argent : vendre un objet, demander un transfert d'argent...

### **4. Contraintes attendues**

Les principales contraintes dans le développement de la monétique en Algérie sont la faiblesse de la bancarisation (la circulation du cash étant prépondérante) et le refus des commerçants à déclarer leur chiffre d'affaires, ainsi que la méconnaissance de l'utilisation de la carte, selon la SATIM.

Pour autant, avec l'initiative d'Air Algérie concernant la réservation et le paiement de billet d'avion électronique, l'utilisation de la carte interbancaire (CIB) n'est pas une garantie pour la compagnie aérienne nationale de voir immédiatement ses clients opter pour cette nouvelle procédure.

## **Conclusion**

Entre le manque de moyens de paiement en Algérie, les attentes vis-à-vis du paiement électronique, les promesses de la SATIM, et les contraintes attendues, le E-paiement devrait faire son entrée avant la fin de l'année courante et Atelcom sera parmi les premiers à avoir fait confiance à cette nouvelle intégration innovante en Algérie.

Malgré tout, le commerce électronique représente un vaste marché qui commence enfin à se développer grâce notamment aux efforts législatifs réalisés ces dernières années et à l'implication des professionnels du monde numérique. Il convient dès lors de consolider cette évolution, qui passe nécessairement par la création de la confiance dans le paiement électronique. Car comme aurait pu dire Monsieur de La Palice au temps de François 1er : « Sans paiement point de commerce ».

## **III. Partie 03 : les techniques de Sécurité**

### **Introduction**

Le commerce électronique, ou le M-commerce, nous présente de nouveaux risques de sécurité. En fait, la propre nature de ce moyen de communication exige un degré significatif de collaboration et confiance entre les acteurs (nœuds) concernés dans des réseaux qui peuvent être exploités par des entités malintentionnées autant pour dénier des services que pour collecter des données confidentielles et ainsi pour disséminer des données fausses.

Une approche globale de la sécurité est essentielle pour défendre le patrimoine d'une entreprise, pour réduire les vulnérabilités des grands systèmes d'information, ou pour protéger sa vie privée.

Cette partie propose un panorama des techniques de sécurité, On propose une approche globale en termes de concepts, de méthodes, et politiques de sécurité.

Cette étude présente les différents aspects de la sécurité : objectifs, menaces, fonctions de sécurité (Internet, réseaux sans fils, GSM,...) Elle aborde les mécanismes de sécurité : cryptographie (chiffrement, signature, protocoles cryptographiques), infrastructure de confiance. Et présente enfin les solutions de sécurité : SSL, IPSec, les VPN,...etc.

# 1. La sécurité et les types de risque dans le commerce électronique

La sécurité est un enjeu majeur des technologies numériques modernes. Réseaux d'infrastructures de télécommunication (GSM, GPRS, UMTS...), réseaux sans fils (Wifi, Wimax,...), Internet, systèmes d'information, Routeurs, Ordinateurs, toutes ces entités présentent des vulnérabilités (failles de sécurité, défaut de conception ou de configuration. Ces systèmes sont attaqués de l'extérieur ou de l'intérieur par des pirates ludiques, des cyber-terroristes,...etc.

Dans ce qui suit nous allons présenter les différents types de risque.

## 1.1 Risques de sécurité et de la vie privée :

La communication sans fil offre une parfaite couverture pour des utilisateurs malintentionnés. Les clients mobiles sont difficiles d'être tracés puisque les PMs vaguent constamment dedans et dehors des zones sans fil, donc des attaques venues des PMs seront probablement les méthodes préférées d'opération pour lancer des attaques contre de réseau fixe, notamment si la capacité de ces PMs s'en accroître.

Le risque de perte ou vol. Un des majeurs problèmes que nous avons avec des PMs aujourd'hui est l'écartement d'un bon mécanisme pour authentifier un client mobile particulier à un PM particulier.

Le risque de vie privée pour nos clients est certain puisqu'on va utiliser leurs numéros de téléphone, ainsi nous aurons un profil clients qui contient l'adresse de livraison, l'année de naissance, leurs préférences pour les divers produits, on va avoir la traçabilité de toutes les transactions et les divers achats effectuer. Ce gisement de données clients va nous permettre de faire de télémarketing pour augmenter les bénéfices de l'entreprise.

Un autre risque correspond à certaines applications qui utilisent de préférences personnelles afin de fournir des services à valeur ajoutée et cela on se sert de notre base de donnée clients qui contient toute les renseignements personnelles, en traçant les divers achats effectuer et en analysant le forum de discussions on peut identifier avec exactitude les besoin de chaque clients. De cette façon les marketeurs peuvent faire de la publicité ciblés, ce qu'implique que ce type de service soit quand même envahissant.

## 1.2 Les risques de la plate forme

La plate forme ou le système d'exploitation utilisé par le périphérique mobile (PM) fournit une infrastructure élémentaire pour l'exécution des applications de m-commerce. En fait sans une infrastructure sécurisée, le m-commerce ne sera pas viable. Malheureusement nombreux manufacturiers de PMs ont faillés en fournir des caractéristiques basiques du système d'opération telles que protection de mémoire pour de processus, contrôle d'accès aux fichiers, authentification des principaux au ressources, privilèges des utilisateurs et des processus, et authentification par biométrie.

## 1.3 Les risques des applications du logiciel

Les failles de logique et implémentation dans le développement d'un logiciel pour des PMs peuvent notamment produire des trous de sécurité qui seront exploités par pirates ou par sites web malintentionnés. Ainsi, par exemple, les langages de bas niveau tels que C ou assembleur nous amèneront toujours des failles élémentaires comme buffer over flow, c'est-à-dire, les logiciels se servent d'un buffer pour stocker en mémoire les données en cours de traitement. Si le pirate connaît l'adresse en mémoire vive, que l'on nomme RAM, de cette mémoire tampon, le buffer du logiciel, il peut provoquer un buffer over flow en dépassant sa capacité maximale de traitement. Les conséquences sont multiples : plantages, fonctions altérées du programme, accessibilités vers des zones normalement réservées.

## 3. Les techniques de sécurité de l'E-paiement

Le rôle des mécanismes et des protocoles de sécurité est d'assurer la confidentialité et l'intégrité de données, et authenticité des parties concernées dans une transaction, en prévenant des périphériques mobiles contre des attaques de dénie de service, filtrage de virus et de code malintentionné, et en quelques cas, de la communication anonyme.

La sécurité mobile (ou sans fil) peut être mieux adressée seulement si elle est prise en considération pendant la conception d'architecture du logiciel (système d'exploitation, logiciel d'application).

Les communications de données mobiles peuvent être sécurisées en employant des protocoles de sécurité qui est ajoutés aux plusieurs couches de la pile du protocole, ou dans l'application elle-même.

### 3.1 Chiffrement (ou cryptage)

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.

#### 3.1.1 Type de Chiffrement

On distingue deux types de chiffrement [SECDEV 09] :

##### a) Chiffrement symétrique

Un procédé de chiffrement est dit "symétrique" si les clés de chiffrement et de déchiffrement sont les mêmes. Le chiffrement symétrique est aussi appelé "chiffrement à clé secrète", puisque cette clé ne doit être connue que par des personnes censées avoir le droit de chiffrer / déchiffrer le message.

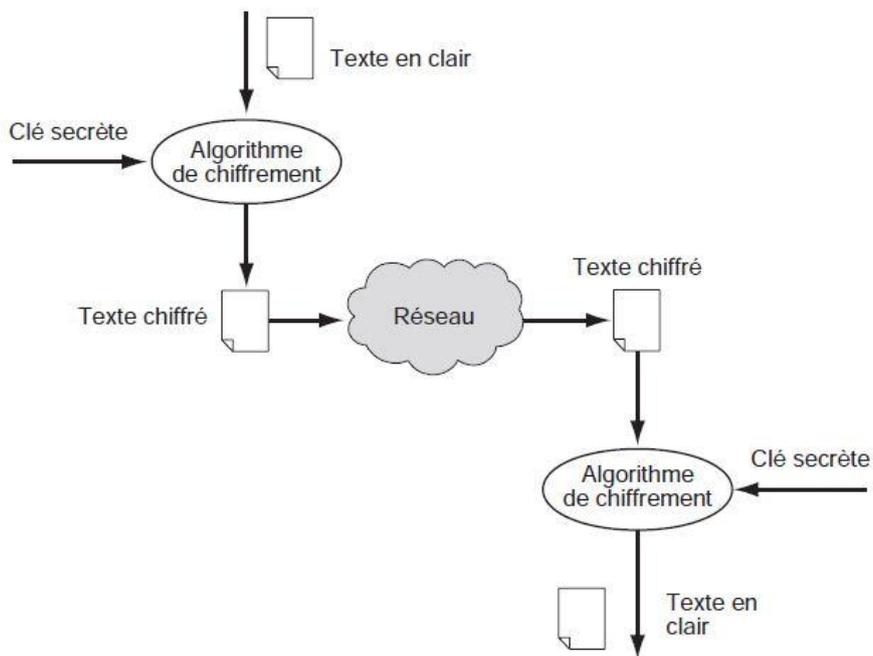


Figure 19. Algorithme de chiffrement symétrique

## b) Chiffrement asymétrique

Le chiffrement asymétrique est aussi appelé "chiffrement à clé publique". En effet, si une personne souhaite que ses correspondants lui envoient des messages chiffrés, elle devra alors générer 2 clés :

- Une première clé servant à chiffrer les messages, qui devra être communiquée à ses correspondants, pour que ceux-ci l'utilisent afin de chiffrer leurs messages.
- Une seconde clé, servant quant à elle au déchiffrement, et qui devra rester privée, afin que seule la personne émettrice des clés puisse déchiffrer les messages.

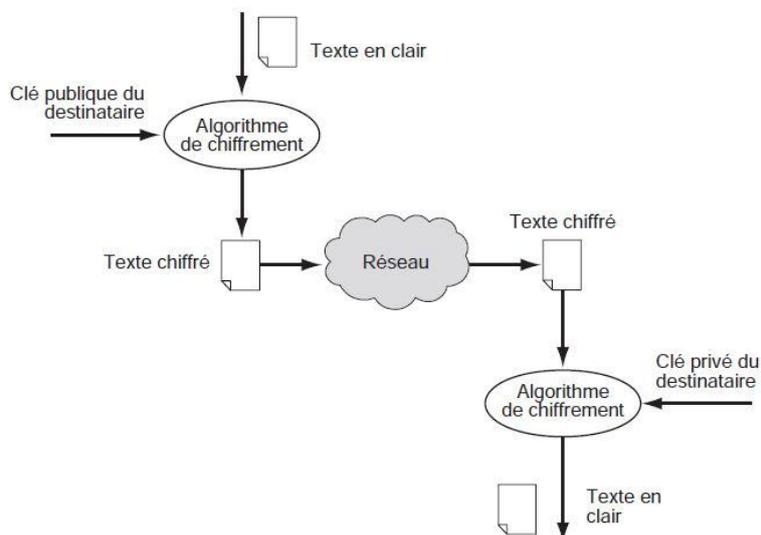


Figure 20. Algorithme de chiffrement Asymétrique

### 3.1.2 Efficacité de la méthode

Un système de chiffrement n'est jamais complètement inviolable ! Il faut même partir du principe que quelque soit l'algorithme employé, trouver une faille ou un moyen de déchiffrer les données protégées n'est qu'une question de temps. Selon la taille de la clé (qui se mesure en bits), il existe un nombre fini de combinaisons qu'un pirate peut essayer pour tenter de déchiffrer le message.

Et la robustesse du système est directement proportionnelle au temps nécessaire qu'il faudrait pour le cracker, donc à la taille de la clé. En résumé, pour qu'un message chiffré soit correctement protégé, il faut que le temps de craquage estimé soit supérieur à la pérennité du contenu du message protégé.

Par exemple, si une information est censée rester secrète un mois, et qu'elle est protégée par un système de chiffrement pouvant résister 5 ans, la sécurité de votre message est en théorie assurée !

Aujourd'hui, il est fréquent d'utiliser des clés de 128 bits dans le chiffrement symétrique, ce qui signifie qu'elle est composée d'une suite de 128 "0" ou "1", ce qui donne  $2^{128}$  possibilités de clés.

Concernant le chiffrement asymétrique, des clés publiques de 1024 bits sont maintenant conseillées, l'opération de déchiffrement ne relevant pas du même procédé que le chiffrement symétrique, il faut dans ce cas utiliser des clés beaucoup plus importantes.

## 3.2 Signature numérique

La signature numérique d'un document électronique à pour vocation de répondre aux mêmes exigences que la signature manuscrite d'un document papier:

- Permettre d'authentifier l'auteur d'un document.
- Garantir qu'une fois signé, le document ne sera plus modifié (falsifié).
- Donner une valeur juridique (sous certaines conditions) au document.

En pratique, une signature numérique est nettement plus fiable qu'une signature manuscrite, puisque cette technologie utilise la technique du chiffrement asymétrique : vous signez numériquement un document à l'aide de votre clé privée, et la lecture du document se fait par l'intermédiaire de la clé publique correspondante, en général transmise avec le document puisque contrairement au chiffrement classique, le but n'est pas de rendre secret le contenu du message.

Ces clés font partie de ce qu'on appelle **un certificat d'authentification** (voir paragraphe suivant) la valeur juridique du document n'est reconnue que si le certificat d'authentification a été fourni par un organisme certifié et agréé. Il existe des logiciels gratuits pour permettre de signer numériquement les documents (le plus connu étant PGP), mais ces documents n'auront donc pas de valeur légale.

### 3.3 Infrastructure à clés publiques (PKI)

Une infrastructure à clés publiques (ICP) ou infrastructure de Gestion de Clés (IGC) ou encore Public Key Infrastructure (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques ou HSM, des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques.

Une infrastructure à clés publiques délivre un ensemble de services pour le compte de ses utilisateurs :

- Enregistrement des utilisateurs (ou équipement informatique).
- Génération de certificats.
- Renouvellement de certificats.
- Révocation de certificats.
- Publication de certificats.
- Publication des listes de révocation (comprenant la liste des certificats révoqués).
- Identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'IGC).
- Archivage, séquestre et recouvrement des certificats (option).

### 3.4 Certificat d'authentification

#### 3.4.1 Définition

« Un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé *autorité de certification* (souvent notée **CA** pour *Certification Authority*).

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire) »

### 3.4.2 Les informations du certificat

Les certificats sont de petits fichiers divisés 3 parties :

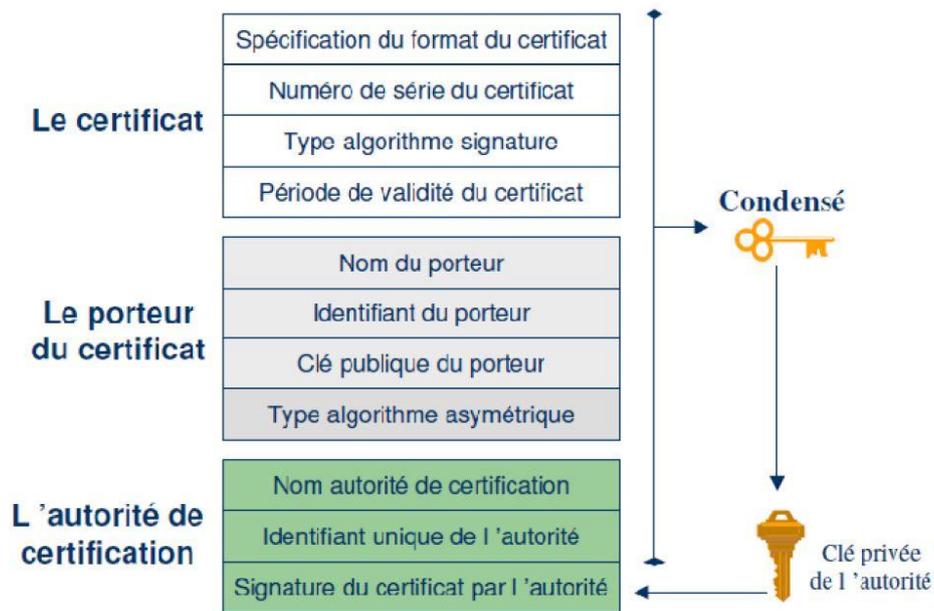


Figure 21. Structure d'un certificat d'authentification

### 3.4.3 L'utilisation des certificats

Les certificats servent principalement dans trois types de contextes :

#### a) Le certificat client

Stocké sur le poste de travail de l'utilisateur (mobile ou fixe) ou embarqué dans un conteneur tel qu'une carte à puce et permet d'identifier un utilisateur et de lui associer des droits.

Dans la plupart des scénarios il est transmis au serveur lors d'une connexion, qui affecte des droits en fonction de l'accréditation de l'utilisateur. Il s'agit d'une véritable carte d'identité numérique utilisant une paire de clés asymétriques d'une longueur de 512 à 1024 bits.

#### b) Le certificat serveur

Installé sur un serveur web, il permet d'assurer le lien entre le service et le propriétaire du service. Dans le cas d'un site web, il permet de garantir que l'URL et en particulier le domaine de la page web appartiennent bien à telle ou telle entreprise. Par ailleurs il permet de sécuriser les transactions avec les utilisateurs grâce au protocole SSL (Voir paragraphe SSL).

#### c) Le certificat VPN

Est un type de certificat installé dans les équipements réseaux, permettant de chiffrer les flux de communication de bout en bout entre deux points (par exemple deux sites d'une entreprise). Dans ce type de scénario, les utilisateurs possèdent un certificat client, les

serveurs mettent en œuvre un certificat serveur et les équipements de communication utilisent un certificat particulier (généralement un certificat IP Sec).

#### 3.4.4 Inconvénients de l'utilisation des certificats

##### a) Complexe :

Les mécanismes d'attribution, de validation et de révocation en font un système très complexe à gérer.

##### b) Pointu techniquement

L'infrastructure à mettre en place (PKI) nécessite une parfaite maîtrise technique.

##### c) Coûts

- Les solutions disponibles sur le marché sont réservées à des applications stratégiques.
- Le coût de déploiement est souvent prohibitif.
- Tendance à sous-estimer les coûts humains de maintenance.
- Le système n'a de valeur que si l'on garantit la parfaite confidentialité, intégrité et disponibilité de la clé privée associée.

### 3.5 Protocole de sécurité dans le paiement en ligne

Nous allons voir les 3 protocoles les plus utilisés dans les solutions de sécurité dans le paiement en ligne

#### 3.5.1 Protocole SSL

##### a) 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. »

« Un serveur web sécurisé par SSL possède une URL commençant par https://, où le "s" signifie bien évidemment secured (sécurisé). Il a été renommé en 2001 **Transport Layer Security** (TLS). Il y a très peu de différences entre SSL version 3 et TLS version 1, TLS diffère de SSL pour la génération des clés symétriques. Cette génération est plus sécurisée dans SSLv3 dans la mesure où aucune étape de l'algorithme ne repose uniquement sur MD5 pour lequel sont apparues des faiblesses en cryptanalyse. Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS. »

## **b) Fonctionnement de SSL**

La sécurisation des transactions par SSL est basée sur un échange de clés entre client et serveur. La transaction sécurisée par SSL se fait selon le modèle suivant :

- ❖ Dans un premier temps, le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier.
- ❖ Le serveur à réception de la requête envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA), ainsi que le nom du crypto système le plus haut dans la liste avec lequel il est compatible.
- ❖ Le client vérifie la validité du certificat (donc l'authenticité du marchand), puis crée une clé secrète aléatoire, chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session).
- ❖ Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peut se faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées.

## **c) Mise en œuvre d'un service HTTPS**

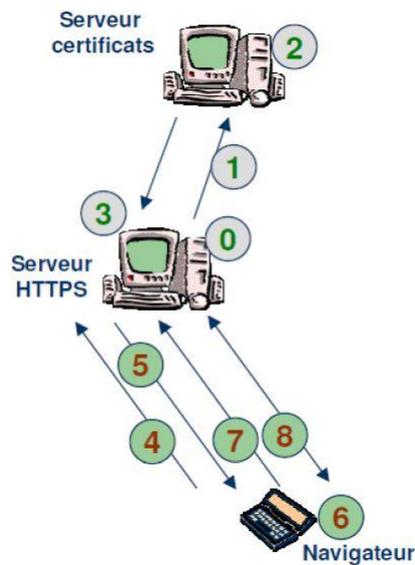


Figure 22. Etapes de la mise en œuvre d'un service HTTPS

#### ❖ 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.echri.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).

Il est à relever que déjà à partir de sa version 2.0, SSL a commencé à être utilisé. Raison pour laquelle encore aujourd'hui, la plupart des intervenants SSL, tentent lors de la phase d'établissement, de dialoguer avec le protocole V3.0, mais si l'un des deux partenaires ne supporte que la version 2.0, et bien c'est cette version antérieure qui va être utilisée. A noter que cette ancienne version contient des clés de cryptage considérées aujourd'hui comme peu sûres.



Figure 23. Site sécurisé dont l'adresse possède le préfixe « https »

Figure 24. Site web non sécurisé

### 3.5.2 Secure Electronic Transactions (SET)

« Le SET (Secure Electronic Transaction) est un protocole destiné spécialement à sécuriser les transactions Internet de paiement par carte bancaire. Il a été développé à l'origine par Visa International et MasterCard, en 1996, avec l'aide des grandes compagnies informatiques de la planète. »

« Son champ d'application se réduit au chiffrement des seules données bancaires, contrairement à SSL qui peut chiffrer les images et le texte. Le protocole SET implique trois parties : le client, le vendeur et la banque du vendeur. Ce système SET requiert des certificats auprès des trois parties. Les certificats du client et du vendeur sont fournis par leur banque respective après quoi la transaction commerciale peut avoir lieu. Avec le SET, le numéro de carte bancaire peut ne pas être connu du vendeur, donc ne sera pas stocké dans ses fichiers et être récupéré par une personne malintentionnée. Le SET assure en principe une transaction de non répudiation, mais cette clause peut varier d'un pays à l'autre suivant la législation en vigueur. »

### 3.5.3 3-D Secure

#### a) Définition

« 3-D Secure est un protocole de paiement sécurisé sur Internet. Il a été développé par Visa pour augmenter le niveau de sécurité des transactions, et il a été adopté par Mastercard. Il permet une meilleure authentification du détenteur de la carte de paiement lors d'achats effectués sur des sites web. 3-D Secure ne doit être confondu ni avec le code secret de la carte bancaire, ni avec le cryptogramme visuel (3 derniers chiffres imprimés au dos de la carte). »  
[ACADRU 09]

## b) Fonctionnement

Le concept de base de ce protocole (basé sur XML) est de lier le processus d'autorisation financière avec une authentification en ligne. Cette authentification est basée sur un modèle comportant 3 domaines (d'où le nom 3D) qui sont:

- Le commerçant (Acquirer Domain en anglais)
- La banque (Issuer Domain en anglais)
- Le système de carte bancaire (Interoperability Domain en anglais)

Le protocole utilise des messages XML envoyés via des connexions SSL (qui garantit l'authentification du serveur et du client par des certificats numériques) .

## c) Mode d'authentification

Le mode d'authentification de notre solution c'est : le client doit s'authentifier avec son numéro de téléphone et un code qui a été déjà envoyé par SMS.

### 3.5.4 Protocole WTLS

Wireless transport Layer Security. Méthode de chiffrement pour les transferts de données entre appareils sans fil, analogue à SSL.

#### 3.5.4.1 Definition

WTLS: Wireless Transport Layer Secure

La couche sécurité vient s'intégrer juste au-dessus de la couche transport de telle sorte qu'elle est située au niveau le plus bas possible, ce qui permet d'assurer grâce à des normes établies, une sécurité meilleure que si elle avait été seulement au niveau applicatif. Le protocole WTLS permet de respecter trois des quatre contraintes principales lorsqu'on parle de sécurité liée aux réseaux :

- 1) **La confidentialité** : Elle assure aux deux parties en présence (mécanisme client serveur) qu'elles sont les seules à avoir accès aux informations échangées. Ceci est assuré par un mécanisme d'encryptions des données.
- 2) **L'intégrité des données** : cela permet de s'assurer que les données n'ont pas été altérées par l'une ou l'autre des parties. On utilise pour cela des algorithmes de hachage pour s'assurer de la validité des données. Il y a une réémission si un changement d'empreinte est détecté d'un coté doté ou de l'autre.
- 3) **L'authentification (coté serveur)**: l'authentification a pour but de prouver qu'un tiers est bien celui qu'il prétend être. Des certificats permettent d'authentifier les serveurs.

Seul le principe de non répudiation n'est pas géré par la couche sécurité : celle-ci aurait pour but de faire preuve juridique qu'une transaction a bien eu lieu. Ce mécanisme est souvent associé à une signature numérique.

On peut penser que les mécanismes de sécurité mis en œuvre nécessitent de grosse puissance de calcul, mais il n'en est rien. WTLS a été pensé de manière à s'adapter aux capacités de calcul et de mémoire limitées et restriction gouvernementale en matière de chiffrement.

Les applications WAP sont capables de sélectionner les besoin de diverse fonctionnalité offerte par WTLS en fonction du niveau de sécurité visée et des caractéristiques du réseau physique de transport. WTLS supporte 3 modes de fonctionnement :

- WTLS Level Class 1 : secret et intégrité.
- WTLS Level Class 2 : secret, intégrité et authentification de la Gateway WAP.
- WTLS Level Class 3 : secret, intégrité et authentification de la Gateway et du terminal WAP

#### *3.5.4.2 Principe de fonctionnement*

La couche sécurité est construite de façon modulaire, c'est-à-dire qu'elle dépend du niveau de sécurité demandé pour ne application donnée. La couche WTLS permet d'avoir une interface pour l'administration des connexions sécurisées. Ce modèle respecte les spécificités définies par TLS 1.0. Les mécanismes mis en œuvre dans cette partie ne seront pas abordés dans les détails, certains étant plus proche de l'algorithmique ou de la cryptographie.

La couche WTLS permet à un client d'établir une connexion sécurisée avec un serveur et de fixer les options de sécurités prises en compte. L'établissement de la connexion sécurisée s'effectue en plusieurs étapes et le client aussi bien que le serveur peut annuler la communication à tout moment. La négociation inclut les paramètres de sécurité, l'échange de clés et l'authentification.

Dans une session pleinement sécurisée, on retrouve un mécanisme similaire à la figure ci-dessous :

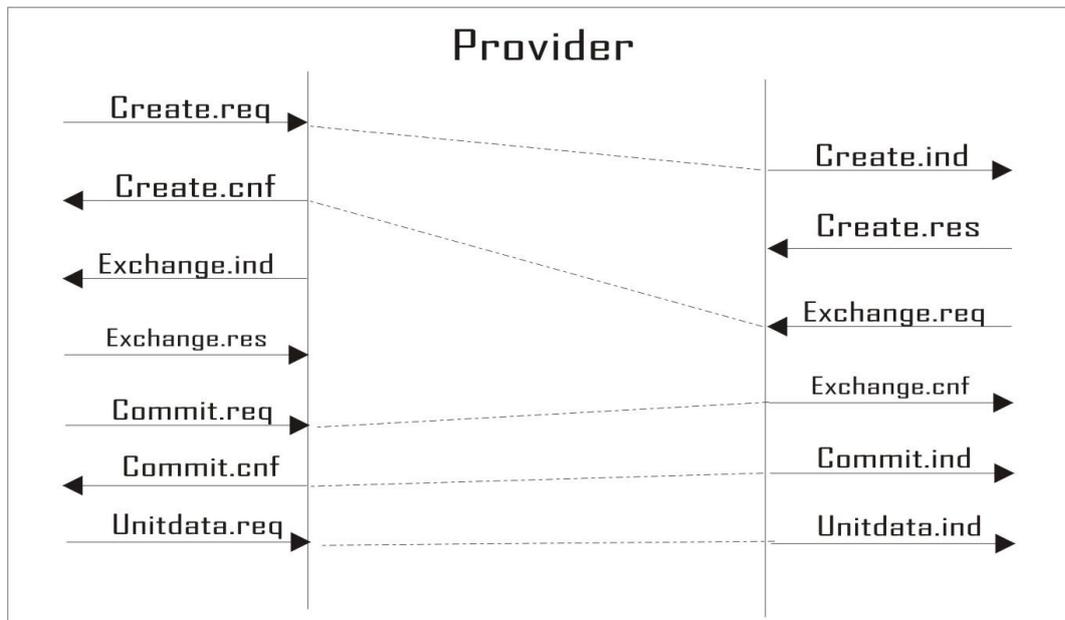


Figure 25. Session sécurisé WTLS

| Nom               | Description                                 |
|-------------------|---|
| Sec-Unit-Data     | Echange d'informations                      |
| Sec-Create        | Création de connexion                       |
| Sec-Exchange      | Echange de clé                              |
| Sec-Commit        | Passage en mode sécurisé                    |
| Sec-terminate     | Mettre fin au mode sécurisé                 |
| Sec-exception     | Avertir d'une exception                     |
| Sec-Creat Request | Demande d'initialisation de part du serveur |

Tableau03. Principe de fonctionnement protocole WTLS.

### 3.5.4.3 Couche enregistrement

Pour réaliser toute opération, la couche WTLS est en fait subdivisée en deux autres couches. L'une est appelée la couche enregistrement, chargée de transmettre les données, éventuellement les compresser, d'appliquer un code d'authentification, de chiffrer et de faire

les opérations inverses pour le déchiffrement. L'autre couche est en fait le protocole d'accord permettant aux deux éléments en présence de se mettre d'accord sur la sécurité mise en jeu.

Une fois que ces paramètres de sécurité ont été échangés et que les clés ont été établies, les états de connexion peuvent être initialisés en leur faisant passer certaines étapes. Pour que la connexion soit maintenue, les méthodes mises en œuvre doivent respecter les paramètres de sécurité définis au dessus, notamment le temps maximal avant une réémission de la clé.

#### *3.5.4.4 Couche de négociation de connexion*

Pour négocier une connexion sécurisée, un protocole d'accord appelé Handshake est nécessaire.

Le protocole Handshake met en œuvre les fonctions suivantes :

- Echange de messages de bienvenue pour un accord entre les deux parties sur les algorithmes utilisés.
- Echange de valeurs aléatoires.
- Echange des paramètres de chiffrement pour permettre au client et au serveur de se mettre d'accord sur une « pré clé de chiffrement ».
- Echange de certificats et des informations chiffrées pour permettre au client et au serveur de s'authentifier.
- Génération de la clé secrète à partir de la « pré clé secrète » et échange de données aléatoires.
- Proposer des mécanismes de sécurité pour la couche enregistrement.
- Permettre au client ou au serveur de vérifier que l'autre extrémité a bien calculé les mêmes paramètres de sécurité et que la négociation s'est bien déroulée sans tentatives d'accès malveillant (hacker).
- 

#### **3.5.5 Protocole SET**

Le protocole SET a été conçu avec l'hypothèse que les utilisateurs effectuent par le biais de terminaux fixes reliés les uns aux autres via des connexions à haut débit. Un terminal typique serait un ordinateur portable ou un PC de bureau capable de réaliser des computations complexes et consommatrices de ressources. De même la disponibilité d'une connexion à haut débit implique qu'une grande quantité d'information peut être échangée entre les différentes parties prenant part à la transaction. Avec la recrudescence du commerce mobile le besoin d'effectuer des transactions SET via des appareils portatifs se fait de plus en plus ressentir.

En effet la grande majorité de ces appareils sont conçus pour fonctionner avec le réseau téléphonique voix, et ont des performances inférieures à celles des ordinateurs conventionnels. Avec l'arrivée des services de troisième génération, on peut s'attendre à ce que SET soit utilisé en commerce mobile de la même manière qu'il est utilisé en commerce électronique mais en attendant le développement des dits services des solutions palliatives doivent être mise en œuvre.

### *3.5.5.1 Définition SET*

SET ou Secure Electronic Transaction, est une technologie qui décrit les algorithmes et protocoles nécessaires pour sécuriser les paiements sur des réseaux publics comme internet. Elle est publique et utilisable par quiconque souhaite sécuriser ses transactions en lignes.

SET a été au départ pour atteindre les objectifs suivants :

- Respecter et préserver la relation Banques-clients.
- Promouvoir le développement du commerce électronique.
- Assurer l'authentification (identification électronique) des porteurs de cartes, des commerçants ainsi que des banques.
- Préserver l'intégrité des données du paiement.

### *3.5.5.2 Schéma d'une transaction basée sur SET*

Le circuit commence par l'émission de certificat. Pour obtenir un certificat, l'acheteur doit impérativement installer un logiciel sur son PC. Une fois le logiciel installé, il doit s'inscrire auprès de l'autorité certifiant de sa banque. Pour ce faire il doit utiliser son logiciel pour transmettre à l'autorité certifiant les informations permettant de l'authentifier ainsi que sa clé publique mémorisée.

En réponse à la demande de l'acheteur, l'autorité certifiant lui transmet un certificat digital. C'est en fait la clé publique de l'acheteur revêtue de la signature digitale de l'autorité certifiant. Une fois émis, le certificat en question ne peut être modifié.

SET n'intervient que lorsque le consommateur souhaite régler le montant d'une transaction. Le logiciel engage alors une conversation avec le serveur du marchand utilisant SET. Une authentification des deux parties a lieu par l'échange des certificats. Ce sont les deux logiciels SET acheteur et marchand qui assurent cette vérification.

L'acheteur fait son choix de produits/services. Le marchand lui envoie un bon de commande accompagné de son certificat. L'acheteur choisit le moyen de paiement qu'il veut l'utiliser, les instructions de paiement sont créées par le logiciel de l'acheteur et envoyées au vendeur cryptées avec la clé publique de l'instruction financière du vendeur. Le vendeur transmet ces informations à son institution financière. Une fois cette information sur le paiement reçue de façon sûre, l'institution financière du vendeur demande une autorisation de l'institution financière de l'acheteur. L'autorisation obtenue, le vendeur confirme la vente de l'acheteur. virement et règlement se font selon les procédures habituelles.

### *3.5.5.3 SET dans le commerce mobile*

Comme le montre la figure du « SET Wallet Server », c'est une approche simpliste équivalente à l'approche SET utilisée dans les transactions conventionnelles. Le logiciel SET client est installé sur un terminal mobile qui a la configuration nécessaire pour réaliser des calculs cryptographiques complexes. L'avantage de cette approche c'est qu'il n'y a aucune modification à apporter au protocole SET original cependant la vitesse de transmission se

dégrade si une grande d'information doit être transférée (pas plus de 9600 bits/seconde dans le cas des réseaux GSM).

#### **3.5.5.4 SET Wallet server**

Contrairement à la première approche SET, Wallet server prend en considération la configuration limitée des appareils portatifs et les limites des réseaux sans fils en termes de bande passante. Le serveur Wallet est une machine fiable, puissante et hautement sécurisée reliée au réseau qui effectue le paiement des transactions sur ordre de l'abonnée. Au lieu d'être placées sur le terminal mobile, les fonctionnalités SET sont centralisées sur ce serveur au même titre que les clés publiques et privées de l'abonnée. La participation du terminal mobile à la transaction est ainsi réduite au strict minimum puisque quelle ne fait que déclencher à distance le processus d'encryptions au niveau du serveur au moyen d'une requête appelée communément Payment Request Message.

A réception de cette requête le serveur Wallet s'engage dans un dialogue avec le serveur du marchand en utilisant les règles habituelles du protocole SET.

L'avantage de cette approche c'est qu'elle permet à l'abonné de se mettre hors ligne en attendant le déroulement de la transaction, ce qui s'avère moins coûteux.

#### **3.5.6 Le protocole HTTPS**

HTTPS est une technique acronyme de protocole de transfert hypertexte sécurisée. Comme son nom l'indique, il est sûr et sécuritaire de la version habituelle http (hyper Text Transfer Protocol).

En HTTPS, le transfert des données est facilité dans une manière plus sûre afin d'éviter les discordances et ingérence inutile et les interceptions de parties non désirés et sans scrupules.

C'est pourquoi, HTTPS est essentiellement idéal pour les transactions de commerce électronique, en particulier des services bancaires en ligne.

Dans l'utilisation de l'HTTPS, les certificats numériques sont cryptés pour garantir la session http sur « Secure Sockets couches » ou SSL est sûr et protégé de l'intrusion extérieure. Au fond, tout autre site Web peut utiliser le protocole HTTPS. Presque tous les types de navigateurs et peut facilement se connecter se connecter à Internet en utilisant soit les protocoles http ou HTTPS.

## **Conclusion**

Nous Avons présenté dans ce chapitre le E-business de manière générale spécialement le E-commerce et E-paiement , ainsi que les différents type et technique de sécurité afin de concevoir un nouveau modèle de E-commerce avec intégration de moyen de paiement électronique sécurisé grâce au différents technique vu dans ce chapitre .

# C

## hapitre 3 :

### Proposer la solution

*« Chacun doit trouver sa solution ». Allen Woody*

## 1. BentschMarking

Pour mener à bien le projet, nous avons fait recours à la technique du Benchmarking afin de proposer la solution de E-paiement adéquate et la plus sécurisée, qui répondra au mieux à notre besoin, tout en tenant compte des technologies existantes issues du domaine de l'E-paiement.

### 1.1 Définition

« Le BentschMarking (en français : analyse comparative) est une technique de gestion de la performance qui consiste à étudier les différentes techniques de gestion et d'organisation des autres entreprises afin de s'inspirer et d'en tirer les meilleurs » [31].

### 1.2 Etude de l'offre du marché

Avant de développer une nouvelle plate-forme de commerce électronique, il est indispensable et très préférable de débiter avec une étude des solutions déjà disponibles sur le marché afin de pouvoir choisir la meilleure solution en termes de coût et fonctionnalités.

Il faut être stratégique avant de créer une nouvelle plate-forme, et notre stratégie c'est de procéder par « BentschMarking », qui consiste à choisir les meilleures solutions et d'en faire une comparaison afin d'extraire les points forts (coût, fonctionnalités, délai, qualité, simplicité...etc.) de chacune pour les adapter à notre solution si le besoin le réclame.

### 1.3 Analyse Comparative

#### 1.3.1 Analyse comparative E-commerce :

Concernant les plates formes E-commerce, il existe plusieurs solutions sur le marché et dans le cadre de notre analyse nous avons choisi les solutions qui nous paraissaient les plus complètes en termes de fonctionnalités ; et pour les sites E-commerce qui existent en Algérie nous allons présenter quelle que uns :

- MADE IN ALGERIA : est site E-commerce, regroupe plusieurs entreprises nationales, ça permet d'orienter les visiteurs du site sur le site de l'entreprise, ou il affiche directement le contact de l'entreprise. Ce qui ressemble vraiment à un annuaire, et il ne permet pas de faire ces chats en ligne.
- Les représentants des grandes lignes d'habillement, on peut citer Puma, Adidas, Nike leurs sites et un site vitrine il permet seulement de visualiser leurs différents produits et ne sont même pas à jour.

## 1.3.2 Analyse comparative E-paiement

### 1.3.2.1 Paiement en ligne par carte CIB

Parmi les solutions étudiées, la seule qui pourra être utilisée pour le paiement électronique en Algérie c'est la carte CB ou appelée en Algérie carte CIB (Carte Inter Bancaire) fournie par la SATIM (Société d'Automatisation des Transactions Interbancaires et de Monétique) commune aux huit banques : BADR, BDL, BEA, BNA, CPA, CNEP, CNMA, Al-Baraka



Figure 26. Carte Interbancaire CIB.

« En Janvier 2010, le paiement en ligne par la carte CIB n'a pas encore eu lieu, mais selon le directeur général de la SATIM, le projet serait en voie de finalisation et subir des tests de faisabilité et performance. Le 1er client étant la compagnie aérienne Air Algérie, les détenteurs de la carte CIB pourront ainsi réserver et effectuer le paiement par internet sur le site web d'Air Algérie, et un code de validation leur sera envoyé.

Selon la même source, on rajoute que ce mode de paiement aussi attendu sera dans les prochains mois élargis à l'entreprise Algérie Télécom pour le règlement des redevances des abonnés à la liaison internet ADSL avant son extensions à d'autres sociétés avec lesquelles la SATIM est en négociation notamment Atelcom. » [32].

La carte CIB rencontre beaucoup de problèmes, et ce qui a ralenti son lancement et cela est due aux :

- Frais de transition très élevé
- Population à 67% non bancarisé
- Absence de communication
- Une économie informelle dominante avec près de 60% des entreprise algérienne.

### **1.3.2.2 Paiement par carte CCP**

En attendant l'entrée en vigueur de la plate-forme de paiement de la SATIM, rien n'empêche les CCP dont plus de 600 millions de clients possèdent une carte électronique, de mettre une plate-forme pour l'e-commerce [33].



Figure 27. Carte de paiement CCP.

- Manque de liquidité (flux monétaire non maîtriser).
- Un service médiocre.
- Retard dans le traitement de demande d'acquisition.
- Elle n'est pas valable pour des transactions qui dépassent les 20.000 DA.

### **1.3.2.3 Paiement par carte visa**

Concernant les transactions financières internationales la SATIM a signé une convention avec la banque de développement local (BDL) pour l'utilisation de la carte visa à compter du mois de juillet prochain [34].

### **1.3.2.4 Contraintes attendues**

Les principales contraintes dans le développement de la monétique en Algérie sont la faiblesse de la bancarisation (la circulation du cash étant prépondérante) population non bancarisé a 67% et le refus des commerçants à déclarer leur chiffre d'affaires, ainsi que la méconnaissance de l'utilisation de la carte, selon la SATIM. Pour autant, l'utilisation de la carte interbancaire (CIB) n'est pas une garantie pour la compagnie aérienne nationale de voir immédiatement ses clients opter pour la nouvelle procédure de réservation et de paiement des billets d'avion.

## 2. Capture des besoins

Tout commence par une volonté politique dans le cadre de l'E-Algérie 2013 vue les avantages promis par le commerce électronique, le gouvernement Algérien veut favoriser les entreprises à se restructurer et à se moderniser dans le cadre de la mondialisation, ainsi avec l'émergence de pousser le consommateur algérien à changer ses habitudes pour remédier aux problèmes de manque de liquidité, et pour le contrôle du flux monétaire. Tout cela dans le cadre de l'E-Algérie 2013.

Le commerce électronique représente un vaste marché qui commence enfin à se développer grâce aux efforts législatifs réalisés ces dernières années et à l'implication des professionnels du monde numérique. Il convient alors de consolider cette évolution, qui passe nécessairement par la création de la confiance dans le paiement électronique.

En ce qui concerne Le site marchand, il est très facile de le créer, il faut juste la liste des produits ou de service que vous proposer, et de sous traiter avec un web designer tout cela pour le prix de 10.000 DA, et voila votre boutique traditionnelle se transforme en boutique virtuelle, mais le problème qui se pose maintenant c'est comment faire pour vendre ?

Nous avons mené notre enquête au prés de plusieurs entreprises et au prés de divers commerçants de proximité, ils étaient tous enthousiastes par l'idée de développer un site vitrine, pour la simple raison d'étendre leurs ventes.

Renouveler son nom de domaine, acheter des fournitures de bureau, payer ses liens sponsorisés, acheter des billets de train ou d'avion pour ses voyages d'affaires... donc s'intéresser seulement a la création des site vitrine ce n'est pas un bon marché .

Mais lorsqu'on veut vendre sur Internet, se pose le problème du paiement électronique sécurisé. Quelle que soit l'activité ou la taille de la société, qu'il s'agisse de biens physiques à livrer, de services ou de produits numériques délivrés en ligne... le moment du paiement en ligne est crucial. Une étude indiquait d'ailleurs il y a quelques temps que 67 % des internautes qui réalisaient leurs shoppings en ligne s'arrêtaient avant la fin de ce dernier, ceci pouvant être lié au manque de choix ou carrément de l'indispensabilité de la solution de paiement c'est pourquoi un chef d'entreprise a mille et une bonnes raisons de recourir au paiement en ligne.

## 3. Notre solution

Notre tache consiste à introduire le E-business en Algérie, tous les donnée que nous avons rassemblé montre que un jour ou autre on doit passer par ce chemin « l'auto route des TIC », et nous devons être les pionniers dans le secteur, et cela seulement avec la conception d'un système innovant et qui en coordination avec les habitudes et la mentalité de l'Algérien.

Pour cette raison qu'on à penser à réaliser un site marchand promotionnel pour crée l'orgueils de mieux acheté et a des prix bas, avec une intégration de notre propre solution de E-paiement.

### 3.1 Un site internet promotionnel

Face à une quasi absence de réels sites de E-commerce en Algérie nous avons eu l'idée de développer un site web promotionnel baptiser « ECHRI » qui présentera toutes les promotions des achats groupés, les bons plans, les soldes de divers produits et de divers secteurs, ou simplement de faire la relation entre les sources des produits et le consommateur final, pour éviter les intermédiaires ce qui rend notre site attractif, et précordial pour tout achat.

Tout cela avec l'option de géo localisation pour identifier le marchand, ainsi notre plateforme ECHRI permettra de gérer les commandes, clients, produits, fournisseurs, marques, livraison...etc.

Notre système a aussi pour objectifs : d'élargir le champ d'intervention en impliquant, tous les internautes dans la plate-forme, en introduisant l'option de notifications personnalisées tout en économisant les ressources de la société (Tâches du personnel, financement de la démarche commerciale...etc.), afin de réduire les coûts et augmenter les revenus.

En plus de notre prospection on a recensé le manque réel d'un comparateur de prix ou un site qui annonce les bons plans, soldes et les promotions. La principale raison c'est que ces derniers sont annoncés par des commerçants de proximité ou des PME qui n'ont pas généralement le moyen de faire de la communication pour leurs promos.

Pour l'objectif d'être le pionnier en matière de vente sur internet, tout en incitant à utiliser notre solution de paiement électronique.



Figure 28. Le logo de notre site marchand ECHRI

### 3.2 La solution de paiement électronique

Précédemment on a vu que les solutions actuelles de paiement électronique sont loin de répondre au besoin du marché, et après plusieurs prospections sur le terrain ainsi que des études faites avec des experts dans la matière, on a capturé tous les besoins du marché ainsi que ces perspectives, ce qui nous a inspiré de trouver notre propre solution et de se placer comme leader dans le marché.

La solution qu'on va élaborer n'est pas l'une des solutions dites « classique » mais plutôt une toute nouvelle plate-forme « moderne » et révolutionnaire dans le sens où elle se sert des nouvelles technologies comme le GSM, GPRS ou le Wifi ; ou alors elles s'adaptent à une demande bien particulière comme les problématiques de micro paiement.

Notre solution c'est un fournisseur de service de paiement électronique que nous avons baptisé « RAHA PAY » pour un premier temps et pour faire notre entrée dans le marché nous avons fourni des comptes prépayés rechargeables par des cartes prépayées de divers montants qui sont faciles à procurer et disponibles partout en Algérie.

Il faut bien sûr suivre l'éthique, notre solution de paiement doit être : flexible, facile et accessible à tout le monde, elle se composera de trois modes de paiement :

- Paiement via internet : nous simplement en proposons un module additionnel à insérer dans un quelconque site de E-commerce.
- Paiement via application Smartphone : en installant une simple application adaptée suivant le téléphone de l'utilisateur et téléchargeable depuis le site de RAHA PAY.
- Paiement via SMS : en envoyant seulement un SMS contenant le code article à notre numéro du serveur SMS.

Les grandes lignes de notre solution de paiement électronique c'est :

- Nous avons choisi d'être un fournisseur de service de paiement mobile (FSPM) seulement pour éviter d'apparaître comme une institution financière.
- Avoir une solution fiable et sécurisée à 100%, qui ne couvre aucun risque.
- Solution simple et attrayante.
- Accessible pour couvrir tout le monde et en tous moments, pour les différentes tranches d'âge, via diverses plateformes d'utilisations.
- Réduire les frais d'utilisation.
- Contrôler et tracer les différentes opérations.
- 

**Justification du choix :**

| Règles  | Le pourquoi ?   |
|---|---|
| <ul style="list-style-type: none"> <li>• Eviter le statut d'une institution financière</li> </ul> | <ul style="list-style-type: none"> <li>• Il nous faut un agrément de la part du ministère des finances ce qui est difficile et lourd pour l'obtenir.</li> </ul> |
| <ul style="list-style-type: none"> <li>• Solution sécurisée</li> </ul>                            | <ul style="list-style-type: none"> <li>• C'est notre atout pour conquérir nos clients, d'ailleurs c'est le pilier de toute solution.</li> </ul>                 |
| <ul style="list-style-type: none"> <li>• Simple à utiliser</li> </ul>                             | <ul style="list-style-type: none"> <li>• Il faut que notre solution soit</li> </ul>   |

|  |   |
|--|---|
|  | attractifs et pour cela il faut qu'elle soit simple et facile pour l'adapter a toute tranche d'âge.   |
| <ul style="list-style-type: none"> <li>• Accessibilité</li> </ul>                              | <ul style="list-style-type: none"> <li>• Il faut diversifier les plate formes d'accès, et l'adapter suivants divers utilisation</li> </ul>  |
| <ul style="list-style-type: none"> <li>• Réduire les frais d'utilisation</li> </ul>            | <ul style="list-style-type: none"> <li>• Il faut modérer les frais d'utilisations au maximum, comme on dit : « la taxe tue la taxe » afin que les gens continue à utiliser notre solution.</li> </ul> |
| <ul style="list-style-type: none"> <li>• Avoir le contrôle sur tous les opérations.</li> </ul> | <ul style="list-style-type: none"> <li>• Il faut éviter toute utilisation malhonnête où frauduleuse, ainsi pour des raisons de traçabilité,</li> </ul>  |

*Tableau04. Justification du choix de notre solution*

## 4. Cahier de charge

### 4.1 Cahier pour site marchand

#### 4.1.1 Objectifs

L'objectif de notre site internet nommé « ECHRI » est bien sur de vendre, on va être les pionniers de l'E-commerce en Algérie car le secteur inexploité, on va introduire la notion de fidélité et du dimensionnement sur mesure suivant le profil de chaque utilisateur, en plus il doit intégrer une partie communication pour le rendre rentable au maximum, Sauf que comme On l'a déjà cité au préalable puisque tous le monde peut crée un site vitrine est vendre, on va se distingué par :

- Collecter tous les importateurs et grossiste et ce qui va nous permettre de proposer les prix les plus bas du marché.
- Intégrer un moteur de recherche.
- Option de Géo-localisation.
- Passer des commandes spécifiques.

### *1.1.1 Cible*

D'après nos études et notre prospection on a déduit qu'on doit cibler :

- un publique majoritairement jeune mais par la suite quand notre mode de paiement sera connu et quand il fera ces preuves notre clientèles sera plus étendu on va cibler les 8 millions d'internaute et les 33 millions d'abonné a la téléphonie mobile notre service sera accessible a 92% de la population algérienne d'ici peu de temps.
- les PME et les commerces de proximité
- les importateurs et les grands distributeurs.
- Les industriels sans exceptions.
- Les grandes surfaces et les centre commerciaux.
- Tous les autres sites de E-commerce qui vont devenir nos partenaires.
- Les sociétés de service qui ont besoin d'intégrer un module de paiement.
- Partenariat avec Sonelgaz , Poste télécom , ADE ....

### *1.1.2 Langues*

Notre solution sera disponible en 3 langues :

- Français
- Arabe
- Anglais
- Ajouter d'autres langues par la suite.

Et Français par défaut, et laisser le choix à l'utilisateur pour définir une autre langue et l'enregistrer dans son profil clients.

### *1.1.3 Aspect et qualité du site*

Tout d'abord notre site sera un site vitrine qui va présente d'une manière virtuel les produits et les caractéristique technique ou informations ainsi qu'un code article sera attribuer pour chaque article.

- Présentation : la présentation du site doit être homogène, claire, concise, simple, intuitive.
- Graphisme : les choix des couleurs doivent respecter la charte graphique, le graphisme doit être doux, fin et ludique
- Interactivité : notre site doit contenir des forums de discussion pour impliqué le consommateur et mieux le comprendre

### *1.1.4 Référencement*

Référencement est un acte primordial pour la vie de tous site internet, et pour cela nous avons fait appel a un expert dans le référencement certifier CESEO, notre site sera référencier dans tous :

- Annuaire et moteurs de recherche français

- Annuaires Algériens, et Google Algérie.
- Annuaires et moteurs de recherche internationaux
- Annuaires et moteurs de recherche par région
- Annuaires et moteurs de recherche de même activité

### *1.1.5 Version mobile du site*

*Un site mobile permet, avec un seul développement, de cibler tous les téléphones du marché, et pas seulement les terminaux haut de gamme de type I Phone, BlackBerry ... Il contribue à accroître la présence de la marque sur le web et à bénéficier d'un référencement plus puissant, plus fin et plus précis. Pour accéder à son compte bancaire, par exemple, un site mobile s'avère parfaitement suffisant.*

## **4.2 Cahier de charge RAHA PAY**

### *4.2.1 Le module RAHAPAY*

Pour que nos partenaire puis adopté notre solution de paiement il faut que nous lui fournirons un module de paiement RAHA PAY

Ce module de paiement est en quelque sorte une redirection vers notre site, la figure suivante représente un aperçu de ce module.

### *4.2.2 L'application mobile*

Notre application, réservée uniquement pour les smart phones, convient à convoiter les utilisateurs les plus actifs, en leur proposant des services supplémentaires. Elle autorise l'accès aux fonctionnalités avancées du terminal (géo localisation, mode non connecté...).

Notre application mobile doit être :

- Compatible : avec tous les types de téléphones mobiles et pour cela il faut la développer pour tous les systèmes d'exploitation mobile (IPHONE, ANDROID, WINDOWS PHONE, SYMBIAN,...), avec de faible besoin en matière de ressources matériel et énergie.
- Simple : une interface simple et ergonomique, nécessite aucun formulaire à remplir ni d'information personnelles à communiquer, c'est le numéro de téléphone de l'utilisateur qui sert d'identification du compte.
- Sécurisé : Paiement sécurisé accès au compte avec un mot de passe et message de confirmation pour chaque opération effectuer .
- Réduire la marge d'erreur dus a la mauvaise utilisation : l'utilisateur si il c'est trompé peut revenir en arrière ou annulé son achats a tous moments.
- Accès restreins : (contrôle parental) pour protéger les mineurs d'accédés a certain contenue ou fonctionnalité.

## 5. RAHA PAY : comment ça marche

### 1er étape :

Le client procure une carte prépayé chez nos partenaires ou chez les buralistes, elle contient un code de 14 chiffres, ce qui lui permet de recharger son compte virtuel à travers notre plate forme de site web, Via une application téléchargé sur son téléphone portable, ou par un SMS.

### 2ème étape :

Le client doit s'enregistrer dans notre service pour bénéficier d'un compte virtuel, son identifiant de compte sera son numéro de téléphone, et un sms lui sera renvoyer en retour pour lui envoyer un mot de passe, qui lui permettra de s'authentifier. Donc chaque client aura un identifiant de compte unique qui est son numéro de téléphone avec un mot de passe.

### 3ème étape :

Chaque client qui est déjà enregistré peut bénéficier de nos services :

- Paiement et achat en ligne.
- Paiement de factures.
- Vérifier l'état de son compte (son solde, ainsi que son historique de paiement qui les a effectués).

Tous cela avec nos 3 modes de paiement (site web, application installé dans le téléphone, via SMS).

## Conclusion

Dans ce chapitre nous avons fait une analyse comparatifs des différentes solutions d'E-commerce et de M-commerce afin d'avoir une longueur d'avance sur tous nos concurrents, et par la suite on à proposer notre propre solution ainsi on a définis les principaux règles pour mieux la cadré et ce qui nous a permis de posé un cahier de charge pour qu'on garde l'éthique de notre solution.

# C hapitre 4 : Réalisation

« Le projet est le brouillon de l'avenir. Parfois il faut à l'avenir des centaines de brouillons ».  
Jules RENARD.

## Introduction

Le but principal de notre projet est de pouvoir acheter et payer via une multiplicité de plate forme fixe comme mobile, comme on l'a déjà vu dans le chapitre précédent.

Dans ce chapitre nous allons s'intéresser au développement d'un site web marchand promotionnel car il va servir comme appât pour l'introduction de notre solution d'E-paiement, et pour cela nous allons développer un module de paiement électronique pour nos partenaires, ainsi qu'une application pour les smart phones.

### 1. Aperçu de notre solution à réaliser :



Figure 29. Architecture de notre solution

## 2. La réalisation du site Web marchand :

On a suivi le cahier de charge, ce qui nous a permis de réaliser la 1<sup>ère</sup> version d'essai, c'est un site plutôt ergonomique qui s'occupe de l'achat jusqu'à la fourniture du produit final avec deux acteurs techniques dans le système, et c'est eux qui bénéficient des fonctionnalités techniques du système :

- ✓ **Utilisateur** : c'est les personnes qui utilisent d'une manière ou d'une autre les fonctionnalités du système.
- ✓ **Administrateur** : c'est la personne chargée de gérer toute la gestion de la plateforme ainsi que de celle des utilisateurs.



Figure 30. Capture d'écran de notre site WEB

### 3. Réalisation du module paiement :

C'est un code prêt à insérer dans n'importe quel site internet, pour que notre partenaire ne trouve aucune difficulté à adopter notre solution de paiement, il lui suffit d'insérer que la ligne de code et le tour est joué.



Figure 31. Module de paiement électronique

### 4. Réalisation des cartes de recharge pour RAHA PAY



Figure 32. Carte de recharge RAHA PAY

Les cartes de recharge RAHA PAY sont générées par une société spécialisée, une carte de recharge RAHA PAY comporte 14 chiffres et un code barre pour la gestion et la sécurité. Elles sont disponibles avec différentes valeurs et chez tous les buralistes et les points de vente des cartes de recharge, pour sa distribution nous allons suivre un chemin qui est déjà tracé par les opérateurs de téléphonie mobile.

## 5. Réalisation de l'application mobile

L'idée de base est d'acheter et de payer ou même transférer de l'argent à n'importe quel moment, depuis n'importe quelle position, vous pouvez ainsi consulter votre solde, l'historique des achats, d'être alerter des nouveau bon plan ou promotion disponible....etc.

### 5.1 Développement sur téléphone portable

Une infrastructure mobile relativement lourde requise dépend d'une multitude de paramètre dont essentiellement la diversité des équipements impliqués.

Pour résoudre ce problème, diverses solutions ont été envisagées par les constructeurs.

Ces solution sont intéressantes mais doivent respecter une certaine stabilité, ce qui n'est pas encore le cas. Actuellement, la solution communément utilisée est Microsoft Visual Studio 2010 Express for Windows Phone

#### 5.1.1 *Qu'est ce que donc Windows Phone ?*

Microsoft Visual Studio Express est un ensemble d'environnements de développement intégrés gratuits développé par Microsoft. Il s'agit d'une version allégée de Microsoft Visual Studio. L'idée de ces éditions "express" est selon Microsoft, de fournir un environnement de développement facile à utiliser et à apprendre pour les développeurs d'applications. La première version de Visual Studio Express (2005) est sortie le 7 novembre 2005 et était supposée n'être gratuite que pour un an (mis à part SQL Server 2005 Express Edition). Toutefois, Microsoft a annoncé que ces éditions resteraient gratuites sans limite de date. <sup>1</sup>

Visual Studio Express est composée de ces différents produits, chacun supportant un seul langage : Visual Basic, C#, C++, J#, Web Developer et SQL Server. Visual J# n'est plus disponible dans Visual Studio Express 2008. L'installation passe par le téléchargement d'un logiciel de moins de 3 Mo qui téléchargera et installera la version de Visual studio choisie (356 Mo pour Visual Basic). Le choix d'installation du répertoire par défaut est défini lors de la première installation d'une des versions choisies (version, langage, etc...).

#### 5.1.2 *Les composants Windows phone*

- Microsoft .NET Framework 4 Client Profile
- Microsoft .NET Framework 4 Extended
- Microsoft .NET Framework 4 Multi-Targeting Pack
- Microsoft Games for Windows - LIVE Redistribuable
- Microsoft Help Viewer 1.0
- Microsoft Silverlight
- Microsoft Silverlight 4 SDK
- Microsoft Windows Phone Developer Resources
- Microsoft Windows Phone Developer Tools CTP - ENU...(Idem)
- Microsoft XNA Framework Redistribuable 4.0

- Microsoft XNA Game Studio 4.0
- Microsoft XNA Game Studio 4.0 Phone Extensions
- Microsoft XNA Game Studio Platform Tools
- Windows Phone 7 Add-in for Visual Studio 2010 - ENU
- Windows Phone Emulator - ENU

### 5.1.3 Choix de Windows Phone : un PC dans le creux de la main

Windows sur un ordinateur, tout le monde connaît, grâce à sa facilité d'utilisation et de sa réputation, le Windows mobile à une longueur d'avance sur tous ces rivaux, Avec les Smartphones sous Windows Mobile, vous ne serez pas dépaycé ! Vous avez l'habitude d'utiliser Internet Explorer pour surfer sur Internet, MSN pour chatter avec vos amis, le pack Office pour travailler, vous voulez retrouver vos contacts Outlook ? Les Windows Phones sont le choix idéal pour retrouver tous ses repères du monde PC en mobilité. Envie de télécharger de nouvelles applications ? Rendez-vous sur Windows Marketplace et téléchargez gratuitement Facebook ou Mappy ou n'importe quelle application qui vous intéresse. [35].

#### Smartphone market share

March '11, Nielsen Mobile Insights, National

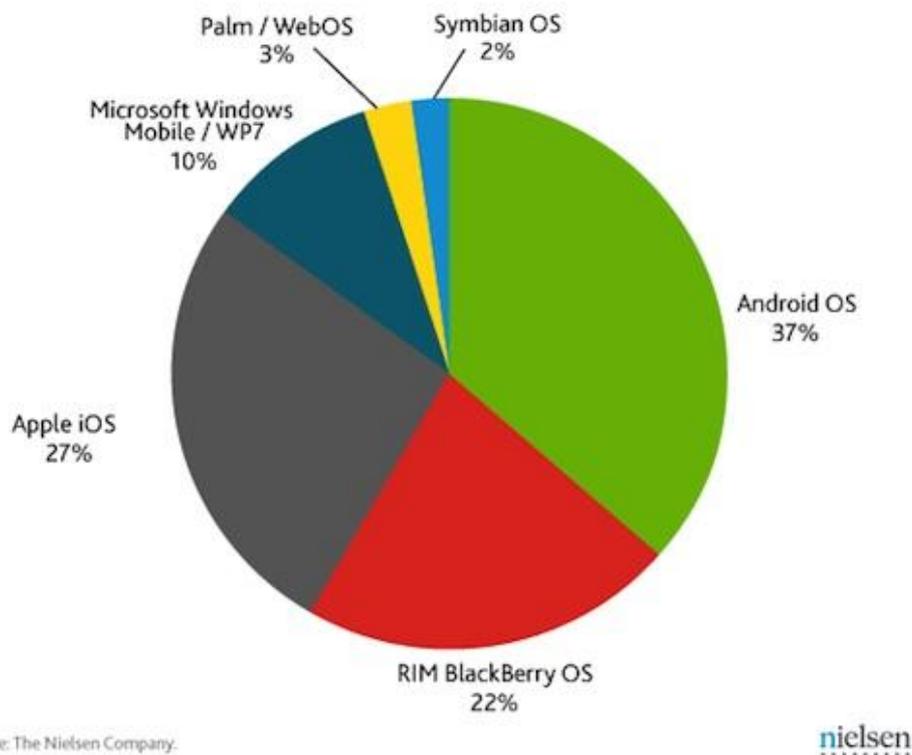


Figure 33 Pourcentage des systèmes d'exploitation mobile

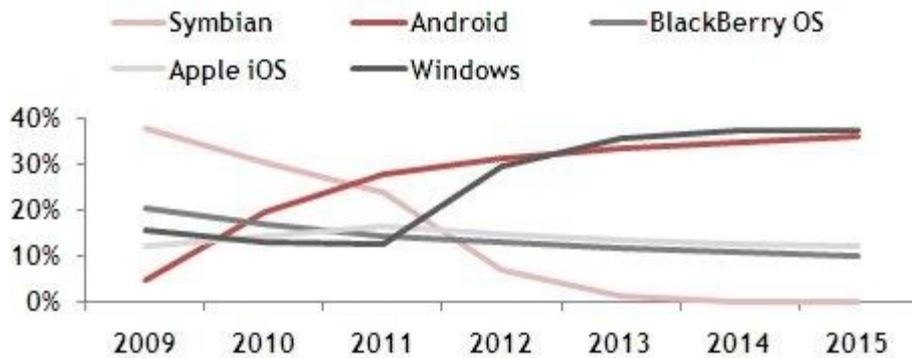


Figure 34. Pr evision pour les syst emes d'exploitation mobile

#### 5.1.4 Condition du fonctionnement

Les conditions de fonctionnement de l'application sont les suivantes :

- Le t el ephone portable doit  tre compatible Windows Phone et GPRS
- L'acc es au r eseau du mobile se fait par GPRS
- 3 Mo d'espace m emoire disponible sur le t el ephone portale

#### 5.1.5 Interface de l'utilisateur final

Pour l'interface de notre application, nous proposons une structure simple   explorer et souple qui permette   l'utilisateur de naviguer facilement entre les diff erentes parties. Donc, un acc es facile aux diff erents sous menus est exig e.

Sachant qu'  tout moment l'utilisateur peut revenir en arri ere jusqu'au menu principal ainsi lui permettre d'annuler ses achats ou sa commande   tous moment.

#### 5.1.6 Ex ecution de l'application :

L'application AutoRun (s'installe automatique) et soit disponible sur notre site Web ou t el echargeable sur Windows Marketplace



Figure 35. Lancement de l'application

Après le lancement de l'application une page de chargement s'affiche pour réserver de l'espace mémoire



Figure 36. 1<sup>er</sup> interface utilisation

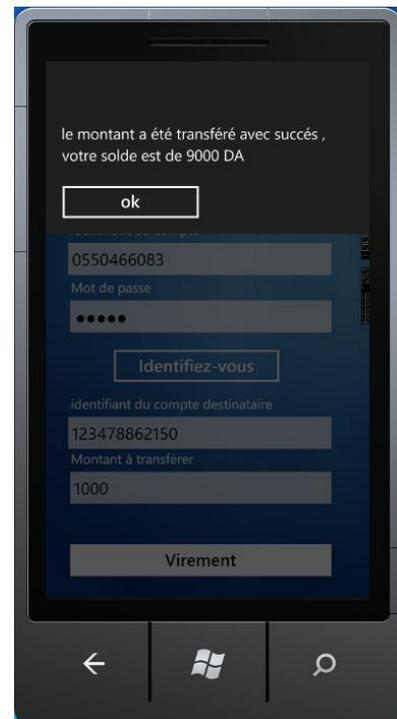
Comme le montre cette capture de l'application il y'a un bouton réservé pour les nouveaux clients qui désirent introduire les numéros de la carte prépayée achetée, ou si l'utilisateur est déjà client il doit seulement cliquer sur le bouton « déjà client » et s'authentifier par la suite.



Figure 37. Services proposé par l'application

Dans le 2eme menu on peut accéder aux différents services proposés par l'application nous avons pris dans ce cas la consultation des bons plans qui fera une redirection pour le site Web mobile, ou la consultation du compte.





*Figure 38. Service de virement compte à compte*

Comme service à valeur ajoutée nous proposons le virement de compte à compte pour les micros paiement ou verser de l'argent à quelqu'un. Il faut juste introduire le numéro de téléphone ou l'identifiant du compte du récepteur. Avec toujours un message de confirmation pour éviter toute erreur d'utilisation



*Figure 39. La consultation du compte*

L'utilisateur peut à tous moments consulter le solde de son compte.



*Figure 40. Détails du compte*

L'utilisateur peut ainsi vérifier l'historique de ses achats, ou procéder par une recherche manuelle suivant la date ex du 23/04/2011 jusqu'au 05/07/2011...

## ***Conclusion***

Le développement d'applications pour mobiles a de beaux jours devant lui. La mobilité devient un facteur clé pour chaque individu dans une société moderne, les téléphones deviennent de véritables petits ordinateurs et offrent des capacités encore sous-exploitées. Nombreux sont les environnements de développement d'applications pour mobile tel que Windows Phone. Ce dernier nous permet de développer des applications à la fois portables, sûres et indépendantes de l'infrastructure des réseaux.

## **Conclusion générale et perspectives:**

- **Conclusion**

Les réseaux sans fil sont devenus un marché porteur en ce début de XXI<sup>e</sup> siècle. Les terminaux téléphoniques mobiles ont été les grands gagnants de la fin du XX<sup>e</sup>, mais ils ne sont dévolus qu'aux communications téléphoniques. Le besoin d'introduire de nouveaux services à fortes valeurs ajoutées sont de plus en plus indispensable dans la société moderne.

Parmi les nouveaux services à valeur ajoutée dans la téléphonie mobile et internet ont trouvé le E-business qui regroupe tout le processus de E-commerce et E-paiement, mais ces services n'ont pas encore fait leurs apparitions en Algérie pour diverses raisons et pour cela on a fait notre prospection sur le terrain et on a décelé plusieurs lacunes qu'ils ont retardé l'apparition de l'E-business en Algérie, alors nous avons pris tout cela en considération et nous avons créé notre propre solution E-business.

- **Perspectives**

Le marché algérien est inexploité, mais avec notre site marchand promotionnel et notre moyen de paiement révolutionnaire, on va conquérir le marché et se placer comme leader, les perspectives qu'ouvrent ce travail est de généraliser le paiement électronique pour étendre notre champ d'intervention introduisant de nouveaux services et techniques de paiement comme le NFC et le NSDT ....etc.

## Référence

- [1] les réseaux, GUY PUJOLLE, septembre 2004, livre de l'édition EYROLLES, page 557
- [2] les réseaux, GUY PUJOLLE, septembre 2004, livre de l'édition EYROLLES, page 577
- [3] les réseaux, GUY PUJOLLE, septembre 2004, livre de l'édition EYROLLES, page 580
- [4] : « téléphonie mobile : GSM, UMTS, 3G, EDGE » [www.guideinformatique.com](http://www.guideinformatique.com)
- [5] handover, roaming, modes de transmissions, high-speed Uplink Packet access  
<http://fr.wikipedia.org/>
- [6] Dossier 3G LTE, un avenir des réseaux mobiles <http://www.generation-nt.com>
- [7] <http://fr.wikipedia.org/wiki/Wi-Fi>
- [8] les réseaux, GUY PUJOLLE, septembre 2004, livre de l'Édition EYROLLES, page 624
- [9] les réseaux, GUY PUJOLLE, septembre 2004, livre de l'Édition EYROLLES, page 626
- [10] technologie client/serveur 2002 <http://fr.selfhtml.org/introduction/internet/standards.htm>
- [11] Fonctionnement du réseau Internet  
<http://www.accreteil.fr/util/programmation/html/html/internet/c-inter2.htm>
- [12] Le modèle TCP/IP par Sylvain <http://www.frameip.com/tcpip/>
- [13] mémoire de fin d'études MOULESSEHOUL Wassila & KRIM Khadidja 2007
- [14] Andrea BAGNOULI « site WAP » 21 déc. 2000
- [15] La revue INSEE PREMIÈRE de l'INSEE N° 771 - AVRIL 2001  
[http://www.insee.fr/fr/themes/document.asp?ref\\_id=ip771](http://www.insee.fr/fr/themes/document.asp?ref_id=ip771)
- [16] (E-commerce : les débuts du commerce en ligne)  
<http://www.e-commerces.eu/e-commerces-debuts.html>
- [17]. (E-commerce : les débuts du commerce en ligne)  
<http://www.e-commerces.eu/e-commerces-debuts.html>
- [18]. La revue INSEE PREMIÈRE de l'INSEE N° 771 - AVRIL 2001  
[http://www.insee.fr/fr/themes/document.asp?ref\\_id=ip771](http://www.insee.fr/fr/themes/document.asp?ref_id=ip771)
- [19]. E-Sens - Web Interface Management - lexique <http://esens.unige.ch/lexique.php>
- [20]. Pourquoi vendre en ligne ? A quoi cela va me servir  
<http://www.buzziessman.com/pourquoivendre-en-ligne/2007/02/21/>
- [21]. ADS-COM, agence Internet Orléans : e-commerce  
[http://www.ads-com.fr/Rub\\_330/Solutionsinternet/e-commerce.html](http://www.ads-com.fr/Rub_330/Solutionsinternet/e-commerce.html)

- [22]. Petite histoire du e-Commerce  
<http://www.x2i.fr/magentoecommerce/petite-histoire-du-ecommerce>
- [23]. Pourquoi vendre en ligne ? A quoi cela va me servir  
<http://www.buzziessman.com/pourquovendre-en-ligne/2007/02/21/>
- [24]. Les 7 briques du e-commerce B to C  
<http://www.superbibi.net/e-commerce/les-7-briques-du-e-commerce-b-to-c>
- [25]. Avantages et inconvénients du cybercommerce  
<http://www.oeconomia.net/private/cours/economieentreprise/themes/ecommerce.pdf>
- [26]. La revue INSEE PREMIÈRE de l'INSEE N° 771 - AVRIL 2001  
[http://www.insee.fr/fr/themes/document.asp?ref\\_id=ip771](http://www.insee.fr/fr/themes/document.asp?ref_id=ip771)
- [27]. La revue INSEE PREMIÈRE de l'INSEE N° 771 - AVRIL 2001  
[http://www.insee.fr/fr/themes/document.asp?ref\\_id=ip771](http://www.insee.fr/fr/themes/document.asp?ref_id=ip771)
- [28]. Avantages et inconvénients du cybercommerce  
<http://www.oeconomia.net/private/cours/economieentreprise/themes/ecommerce.pdf>
- [29]. Le quotidien d'Oran 18/05/2011 les aveux du ministre
- [30]. Benchohra KARA Le commerce électronique en Algérie : défis et perspectives Mémoire de fin d'études INPS  
[http://www.memoireonline.com/07/08/1195/m\\_commerce-electronique-algerie-defisperspectives-cas-satim5.html](http://www.memoireonline.com/07/08/1195/m_commerce-electronique-algerie-defisperspectives-cas-satim5.html)
- [31]. Benchmarking (benchmarking) <http://pfeda.univ-lille1.fr/iaal/b.htm>
- [32]. Algérie Poste Services Financiers: La monétique  
<http://www.poste.dz/sf/?page=monetique&idc=30> mars10
- [33]. Algérie Poste Services Financiers: La monétique  
<http://www.poste.dz/sf/?page=monetique&idc=30> mars10
- [34]. Algérie Poste Services Financiers: La monétique  
<http://www.poste.dz/sf/?page=monetique&idc=30> mars10
- [35]. Choix de Windows Phone [http://www.microsoft.com/windowsphone/fr-fr/default.aspx?WT.mc\\_ID=wpvan](http://www.microsoft.com/windowsphone/fr-fr/default.aspx?WT.mc_ID=wpvan)
- [36]. Les solutions de paiement sur Internet  
<http://www.abcnetmarketing.com/Introduction,1842.html>
- [37]. Les moyens de paiement en ligne  
<http://www.commentcamarche.net/faq/sujet-9668-les-paiements-en-ligne>

## **Résumé**

L'essor fulgurant de l'Internet et le développement des technologies de l'information et de la communication (TIC) ont généré de nouveaux besoins en termes de nouveau service à valeurs ajoutées afin d'améliorer le quotidien, pour l'individu comme pour les entreprises qui cherchent à se moderniser.

Une société qui propose des produits et/ou des services, cherche toujours à adopter la meilleure solution afin de pouvoir rivaliser sur le marché qui ne cesse d'augmenter la concurrence. C'est l'objectif de notre projet qui consiste à mettre en place une plate-forme de commerce électronique sur le web avec un système de paiement électronique intégré.

Notre système a aussi pour objectifs : d'introduire la notion d'E-business, d'élargir le champ d'intervention en ciblant les 8 millions d'internaute et les 33 millions d'abonnées en téléphonie mobile.

Afin de développer notre système, nous avons choisi d'être un fournisseur de solution de paiement électronique en proposant notre module de paiement flexible à toutes les entreprises qui veulent proposer leurs produits ou services, en lui offrant le choix et la mobilité d'acheter et de payer via une multitude de plate forme.

## **Abstract**

The explosive growth of the Internet and the development of information technology and communication have created new needs in terms of new value added to improve the lives for the individual as companies seeking to modernize.

A company that offers products or services, always looking to adopt the best solution in order to compete in the market is increasing competition. This is the goal of our project to build a platform of electronic commerce on the web with an integrated electronic payment system.

Our system also has the following objectives: to introduce the concept of E-business, to expand the scope of action by targeting the 8 million and 33 million Internet subscribers in mobile telephony.

In order to develop our system, we choose to be a provider of electronic payment solution offering is our flexible payment module to all companies that want to offer their products or services, by offering choice and mobility to buy and to pay via a variety of platform.