Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABOU BAKR BELKAID –TLEMCEN
FACULTE DE TECHNOLOGIE
DEPARTEMENT GENIE ELECTRIQUE ET ELECTRONIQUE
LABORATOIRE LTT

MEMOIRE
Pour l'obtention du

DIPLOME DE MASTER EN
RESEAUX ET SYSTEMES DE TELECOMMUNICATIONS

Thème :

Conception et réalisation d'une solution Multi-Communications pour la gestion de CCP

Présenté par :
Mr HAMEL Hocine
Mr BARKA Mohammed

Soutenu le 26 Juin 2013 devant le jury composé de :

Président	:	Mr N. BENAHMED	Prof, Université de Tlemcen
Examinateur	:	Mr M. CHIKH-BLED	Prof, Université de Tlemcen
Examinateur	:	Mr R.BOUABDALLAH	MAA, Université de Tlemcen
Encadreur	:	Mr M.BOUSAHLA	MCB, Université de Tlemcen
Co-Encadreur	:	Mr M.ROUISSAT	Doctorant, Université de Tlemcen

Année universitaire 2012/2013

Remerciement

Nous tenons avant tout à remercier Dieu tout puissant de nous avoir donné la force et la volonté pour achever ce modeste travail.

Nous tenons à remercier particulièrement nos parents ; notre succès demeure de loin le fruit de leurs longues années de sacrifices et d'éducation.

Nos vifs remerciements, accompagnés de toute notre gratitude, vont tout d'abord à notre encadreur Mr M.BOUSAHLA, pour nous avoir proposé ce sujet et dirigé notre travail, Mr M.ROUISSAT, pour son prestigieux aide, sa disponibilité et avis éclairés.

Nous remercions également Mr N.BENAHMED, Professeur à l'université de Tlemcen pour avoir accepté de présider le jury.

Nous adressons nos remerciements à Mr M.CHIKH-BLED, Professeur à l'université de Tlemcen et à Mr R.BOUABDELLAH, Maitre-assistant à l'université de Tlemcen pour l'intérêt qu'ils ont bien voulu porter à ce travail en acceptant de faire partie du jury.

Nous ne pouvons-nous empêcher d'avoir une pensée pour ceux et celles qui ont répondu présents et nous ont offert leur soutien moral dans les moments difficiles et qui étaient à nos côtés pour partager avec nous les moments de joie.

Dédicaces

Je dédie ce modeste travail à mes très chers parents qui n'ont pas cessé de m'encourager durant toutes mes études que dieu me les garde ;

Ma grand-mère qui je souhaite une longue vie ;

À mes frères, mes sœurs

À mes cousins et cousines et tous ceux que j'aime ;

À mes amis, Abdelmounaim, Zakia, Saadi, Tarek, Ismail, Ibrahim, et toute la promotion RST

Ainsi qu'à toutes les personnes qui nous ont aidés à la réalisation de notre travail.

Mohammed

Dédicaces

Je dédie ce modeste et mémorable travail, plus particulièrement à mes aimables et respectueux ***parents*** *qui m'ont accompagné dans toute ma vie, s'inquiétant énormément pour m'offrir une vie meilleure. Je tiens la parole pour leur dire :* ***« Voilà les fruits de vos sacrifices !».*** *Que Dieu vous protège !*

À mes frères, ma sœur

À mes cousins et cousines et tous ceux que j'aime ;

À Khaled ;

Je tiens aussi à saluer tous mes amis et en particulier : ***Tarek, Ismail, Ibrahim, Benamar, Imad, Djamel, Fouzi, Mahmoud, Abdelmonaim****. Ainsi que tous la promotion RST.*

Hocine

Résumé

L'explosion du nombre de terminaux mobiles dans le monde, au point de dépasser celui des ordinateurs, est un fait économique important. Avec les nouveaux réseaux de télécommunication et l'accroissement des capacités de traitement des terminaux, de nouvelles possibilités d'interagir et de communiquer avec les clients, y compris via le réseau Internet, ont fait leur apparition. Ainsi, l'Internet Mobile apporte des opportunités d'élargissement de la palette des services proposés par les banques.

L'amélioration de ces techniques électroniques du système bancaire a pour but de faire face aux défis de l'ère moderne, et assure la circulation des services bancaires avec une grande efficacité.

L'objectif de ce mémoire concerne la conception et la réalisation d'une solution Multi-Communications pour la gestion de CCP.

Trois solutions ont été proposées dans ce mémoire : Un site web (E-Banking), une application J2ME (M-Banking) et un service de SMS-Banking, ce qui donne aux clients la liberté de consulter leurs comptes et faire quelques autres opérations bancaires, par le service qui leur convient.

Sommaire

Listes des Figures

Introduction générale

Introduction générale

Les innovations dans les technologies de l'information et de la communication (TIC), adossées à la globalisation de l'économie mondiale ont induit une accélération de mouvements de capitaux telle qu'elle requiert des systèmes transactionnels modernes et efficaces visant à sécuriser et harmoniser ces importants flux financiers. Le développement des applications de paiement par voie électronique qui vient se substituer progressivement à l'échange physique des moyens de paiement, constitue une des réponses bancaires à cette logique visant à plus de sécurité, plus d'efficacité , plus de fluidité et de rapidité.

L'activité bancaire a effectivement connue une mutation importante en matière de distribution des services. Aux développements et perfectionnements des automates bancaires (AB) et serveurs vocaux (SV) sont venus ajouter l'offre de services par Internet. L'agence n'est plus, comme autrefois le canal de distribution exclusif de la banque. Ainsi les distributeurs automatiques de billets (DAB), les guichets automatiques de banque (GAB) et Internet ont fait successivement voler en éclats l'unité de lieu, de temps et d'action, principe si cher aux institutions bancaires. L'objectif étant d'ajouter le plus d'éléments de satisfaction (niveau de confort ressenti par l'utilisateur) possible en vue de fidéliser une clientèle par ailleurs « volatile » du fait d'une concurrence farouche entre établissements.

Le potentiel qui s'ouvre aux banques pour contacter leur clientèle n'a jamais été aussi vaste ; et les enjeux sont à la hauteur :

- forte fidélisation des clients.
- réduction significative du coût des prestations à faible valeur ajoutée.

Par ailleurs, Internet réduit significativement le coût d'entrée d'un nouvel arrivant qui peut viser des créneaux spécifiques du marché bancaire ; des services nouveaux peuvent être proposés.

Parmi les services on propose trois solutions dans ce mémoire :

- Un site web (E-Banking).
- Une application J2ME (M-Banking).
- Un service de SMS-Banking.

Ceci donne aux clients la liberté de consulter leurs comptes et faire quelques autres opérations bancaires, par le service qui leur convient.

Le présent mémoire est organisé en quatre chapitres dont nous donnons une brève description dans les lignes suivantes :

Le premier chapitre est consacré à la présentation des différents services d'E-Banking et à une description du réseau GSM qui est le moyen de communication entre le client et le serveur (M-Banking). Ce chapitre se conclura par une présentation de quelques services d'E-Banking en Algérie.

Le deuxième chapitre concerne la présentation de l'accès à l'internet, les protocoles utilisés, la cryptographie et la technologie WAP.

Dans le troisième chapitre, nous présentons les différents langages de programmation utilisés dans la réalisation de nos applications (PHP, HTML, J2ME, PYTHON, NETBEANS, WAMP, NOTEPAD …).

Le dernier chapitre contient la présentation de nos applications (site web, application J2ME, serveur SMS).

Enfin, ce document se termine par une conclusion générale et une bibliographie qui comprend les références des ouvrages et les ressources Web relative à notre travail.

Chapitre I E-Banking et réseaux mobiles

I.1. Introduction

Dans ce chapitre introductif, nous présentons des généralités sur l'E-Banking, L'architecture du réseau GSM, qui est le moyen de communication entre le client et la banque (cas de M-Banking) et l'E-Banking en Algérie.

I.2. Présentation d'E-Banking

L'E-banking ou encore le (Inter) net Banking, Web Banking ou Online Banking signifie « La banque sur Internet ». Tous ces termes désignent l'utilisation de l'Internet par une institution financière en vue d'offrir à ses clients une gamme de services bancaires plus ou moins larges, allant de la simple vitrine commerciale à la gestion à distance de transactions financières.

E-Banking ou banque électronique désigne donc le fait de se servir d'un outil électronique, comme l'ordinateur, pour effectuer les différentes transactions bancaires.

L'E-Banking permet l'accès aux comptes, le transfert de fonds d'un compte vers un autre, l'information sur le solde, le transfert de fonds vers le compte d'un tiers, le paiement de factures, etc. Les possibilités sont nombreuses et permettent d'économiser beaucoup de temps aux gens qui utilisent ces services. [1]

Parmi les services d'E-Banking :

- L'Internet Banking.
- Le guichet Automatique Bancaire (GAB).
- Le Mobile Banking
    - Le WAP Banking
    - Le SMS Banking

La figure suivante montre les services d'E-Banking

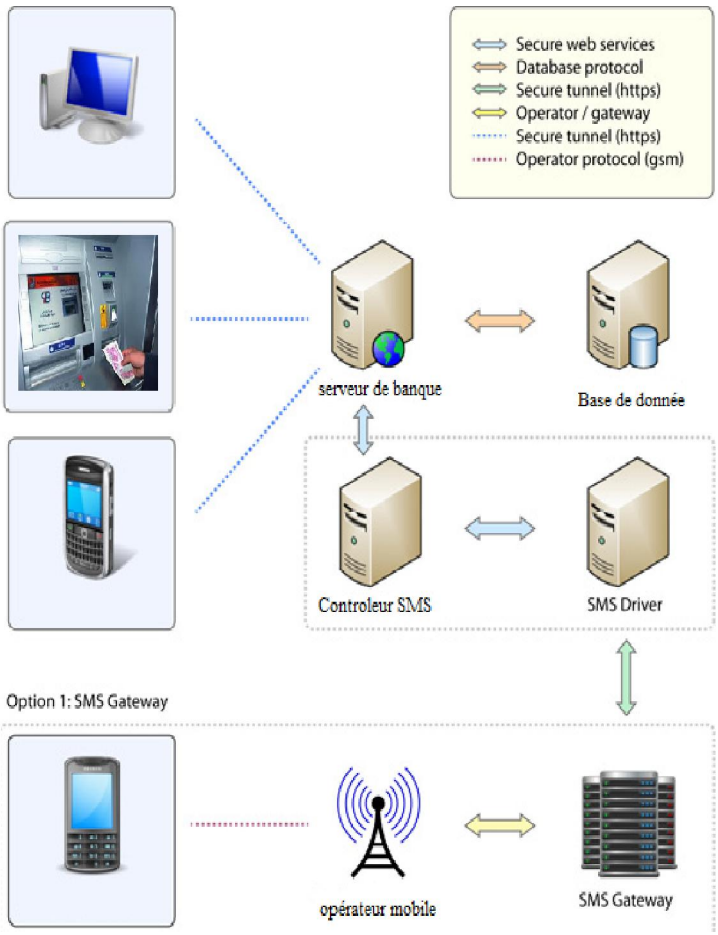


Figure I-1: Architecture générale d'E-Banking

I.3. Les services d'E-Banking

I.3.1. L'internet Banking

Est un système permettant aux individus d'exercer des activités bancaires à la maison, via internet. Certaines banques en ligne sont des banques traditionnelles, qui offrent également des services bancaires en ligne, alors que d'autres sont en ligne n'ont aucune présence physique.

Les services bancaires en ligne, par l'intermédiaire de banques traditionnelles permettent aux clients d'effectuer des transactions de tous les courantes, tels que les transferts de comptes, demandes de solde, paiement de factures et demandes d'arrêt de paiement, et certaines banques offrent même des demandes de prêt et de carte de crédit en ligne.

Quelques banques en ligne mettent à jour les informations en temps réel, tandis que

d'autres le font tous les jours. [2]

I.3.2. Guichet Automatique Bancaire(GAB)

Est un automate permettant au détenteur d'une carte bancaire d'effectuer de nombreuses opérations sans intervention du personnel de sa banque et ce 24 H sur 24 H. L'utilisation d'un GAB permet aux clients de l'établissement propriétaire du GAB, notamment, d'effectuer les opérations suivantes : consultation de solde, demande de RIB, demande de chéquiers, virement de compte à compte au sein de la banque, remise de chèques, versement d'espèces, retrait d'espèces. Les GAB font aussi fonction de distributeurs de billets (DAB) pour l'ensemble des porteurs de cartes acceptées par l'appareil. [3]

Figure I-2 : Exemple d'un GAB

I.3.3. Le M-Banking

Le Mobile Banking est l'utilisation du téléphone portable « mobile phone » pour fournir des services bancaires qui peuvent être des transactions financières et des échanges d'informations entre le client et l'institution financière.

Le Mobile Banking est un moyen de communication utilisant le téléphone portable qui s'est très fortement répandu ces dernières années, pour :

- Faciliter l'accès aux services bancaires ;
- Diversifier et améliorer l'offre de services bancaires auprès de la clientèle ;
- Réduire les coûts de transaction pour les clients dans les zones éloignées ;

Le Mobile Banking réunit les 2 applications 'SMS Banking' et 'WAP Banking' [4]

I.3.4. WAP Banking

Le WAP Banking permet d'accéder au compte bancaire par l'intermédiaire de l'Internet mobile.

La sécurité des transactions effectuées par ce procédé est traitée tout comme la sécurité d'application web, avec l'envoi d'informations chiffrées depuis le mobile. Cette forme d'opérations mobiles convient aux combinés de modèles récents qui soutiennent les technologies WAP, GPRS, 3G ou EDGE.

Cette technique peut être déployée de deux façons : [5]

- Soit par site web réparti entre la carte SIM du client et le serveur de la banque (certaines pages web logent dans la carte SIM du client) ; à cet effet les informations fournies sont envoyées via une connexion Internet vers le serveur de la banque qui les traite et renvoie le résultat.
- Soit par site web centralisé au niveau du serveur de la banque ; à cet effet le client établit une connexion Internet entre le serveur web du client et sa carte SIM avant toute sollicitation de service.

La figure suivante montre le fonctionnement de WAP Banking

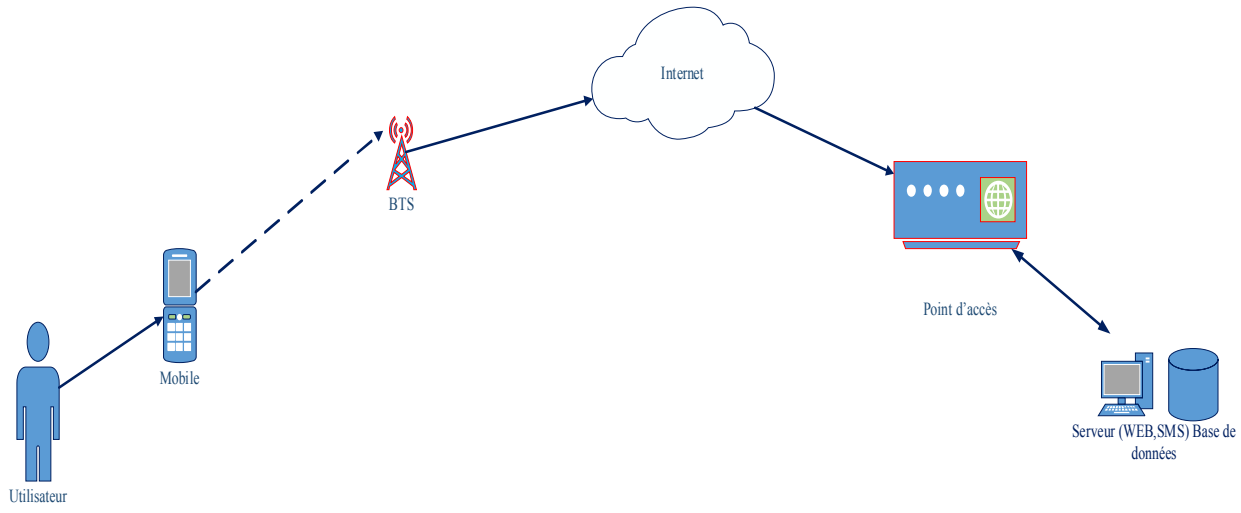


Figure I-3 : Illustration du fonctionnement d'un wap banking

I.3.5. SMS Banking

Le SMS-Banking est une branche de l'E-Banking qui combine le SMS et le téléphone mobile. A ce titre, Les clients de la banque peuvent gérer leur compte, visualiser leurs soldes, demander des chéquiers, faire des virements, payer des factures et d'autres transactions bancaires en utilisant leur téléphone mobile.

La figure suivante illustre de façon globale le fonctionnement d'un SMS Banking. [1]

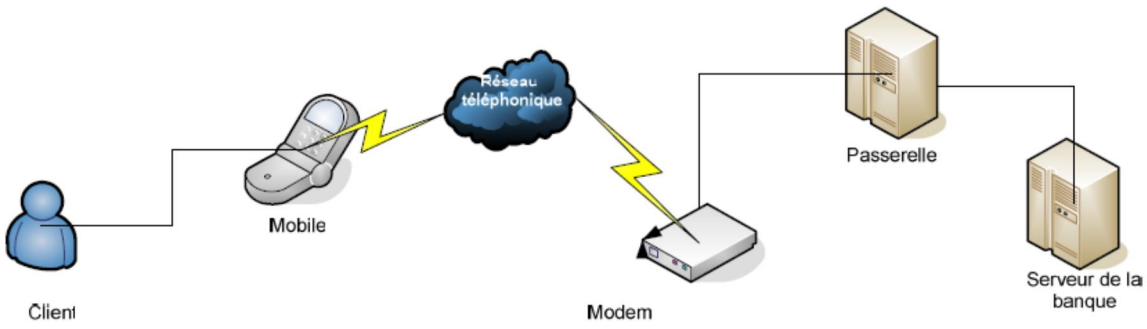


Figure I-4 : Illustration du fonctionnement d'un SMS-Banking

I.4. Le réseau GSM

I.4.1. Présentation

Le réseau GSM (Global System for Mobile communications) constitue au début du 21ème siècle le standard de téléphonie mobile le plus utilisé en Europe. Il s'agit d'un standard de téléphonie dit « de seconde génération » (2G) car, contrairement à la première génération de téléphones portables, les communications fonctionnent selon un mode entièrement numérique. Fondé en 1989, l'Institut européen des normes de télécommunication (ETSI) a été chargé d'élaborer la norme GSM.

Le GSM 900 utilise la bande 890-915MHz pour l'envoi des données et la bande 935-960 MHZ pour la réception des informations.

Le GSM 1800 utilise la bande 1710-1785 MHz pour l'envoi des données et la bande 1805-1880 MHz pour la réception des informations. [6]

I.4.2. Architecture

La figure suivante montre une architecture générale du réseau GSM.

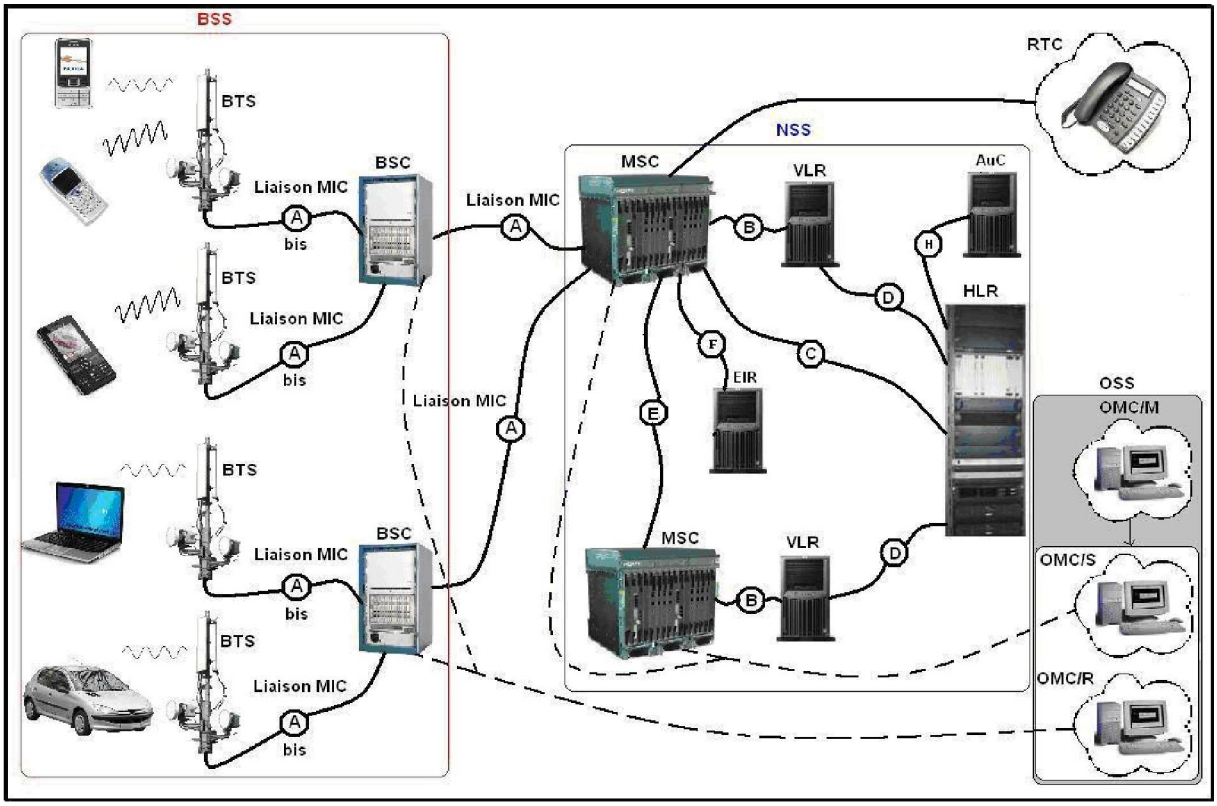


Figure I-5 : Architecture générale de GSM

Le réseau GSM est constitué de cellules adjacentes (figure I-6) au sein desquelles les ondes hertziennes sont reçues et retransmises par des BTS. Ces ondes sont des canaux porteurs de la voix ou des données ou encore d'informations de signalisation.

Pour cela, il est constitué principalement de deux parties, l'une mobile et l'autre fixe, communicant par l'intermédiaire d'un lien radio, généralement appelé interface air (ou plus rarement interface Um).

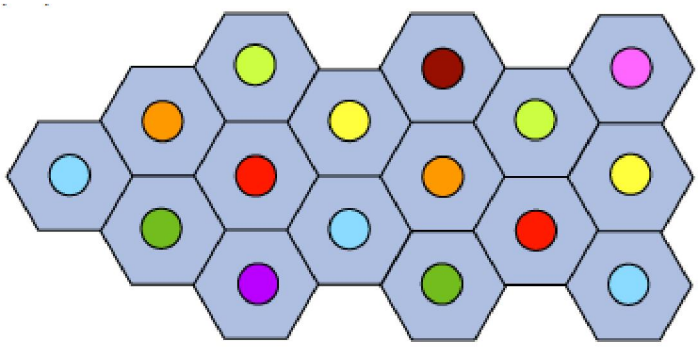


Figure I-6 : Les cellules dan le réseau GSM

La partie mobile appelée station mobile (MS) concerne [7]

- Les terminaux (appareils), identifiés par un numéro unique appelé IMEI (International Mobile Equipment Identity), qui sont des supports de carte SIM.
- La carte SIM possède un numéro d'identification unique (et secret) appelé IMSI (International Mobile Subscriber Identity). Elle permet ainsi d'identifier chaque utilisateur, indépendamment du terminal utilisé lors de la communication avec une station de base.

La partie fixe est elle aussi subdivisée ainsi :

- Le BSS (Base Station Subsystem) : sous-système radio constitué de contrôleur de stations (BSC) qui gère la répartition des ressources et les stations de base (BTS) qui lui sont reliées.
- Le NSS (Network Station Subsystem) : ensemble des connexions physiques reliant les BSC, le OMC et le MSC (Mobile Switching Center), géré par l'opérateur téléphonique.

La zone du commutateur (MSC) est généralement reliée à des bases de données assurant des fonctions complémentaires :

- Le registre des abonnés locaux (noté HLR) contient des informations (position géographique, informations administratives, etc.) sur les abonnés de la MSC.
- Le registre des abonnés visiteurs (noté VLR pour Visitor Location Register) qui contient des informations sur les utilisateurs autres que les abonnés locaux. Le VLR renvoie les données vers un nouvel utilisateur à partir du HLR correspondant à sa zone d'abonnement.
- Le registre des terminaux (noté EIR pour Equipement Identity Register) qui répertorie les terminaux mobiles.
- Le Centre d'authentification (noté AUC pour Authentification Center) chargé de vérifier l'identité des utilisateurs.

Le SMSC permet de gérer le transfert de messages SMS (textes ou binaires) entre téléphones mobiles.

Le réseau cellulaire ainsi formé est prévu pour supporter la mobilité grâce à la gestion du passage d'une cellule à une autre ainsi que le passage du réseau d'un opérateur à un autre.

Le standard GPRS (General Packet Radio Service) est une évolution de la norme GSM

qui permet le transfert de données par paquets. Grâce à ce mode de transfert, les transmissions de données n'utilisent le réseau que lorsque c'est nécessaire et l'utilisateur est facturé au volume échangé plutôt qu'à la durée de connexion. Ainsi, le standard GPRS utilise l'architecture du réseau GSM pour le transport de la voix, et propose d'accéder à des réseaux de données (notamment Internet) utilisant le protocole IP ou le protocole X.25.

I.4.3. Acheminement de message

Les messages sont acheminés directement sur un canal de contrôle. Initialement, le canal de transit des SMS, avait été conçu pour la transmission de messages de maintenance de l'opérateur vers les exploitants du réseau ; et progressivement le SMS a été configuré pour la communication entre les abonnés. L'acheminement entre les divers équipements du réseau est géré par le protocole MAP. [8]

L'envoie d'un message d'un mobile à un autre se passe en deux étapes :

- Le message part du terminal vers le SMSC (étape qualifiée de SMS-MO).
- Le message est ensuite envoyé du SMSC vers le mobile destinataire.

I.4.4. Mécanismes de sécurité dans le GSM

La sécurité du réseau GSM repose sur des mécanismes cryptographiques non publiés et utilisent d'une part un code enregistré dans la carte SIM : le code IMSI (International Mobile Subscriber Identity) ; d'autre part un code unique composé de 15 chiffres qui identifie le MS : le code IMEI qui est stocké dans le EIR. (Sur la plupart des mobiles, le code IMEI peut être obtenu en entrant la séquence *#06#). Le MS fonctionne uniquement si l'IMSI et l'IMEI sont valides. [1]

D'autant plus, une clé secrète Ki (Subscriber Authentication Key) est attribuée par l'opérateur téléphonique utilisée en cryptographie dans toutes les fonctions sécurisées, elle est stockée dans le ASC et elle est préinstallée dans la carte SIM par l'opérateur. [Gsm 02]

L'authentification de l'abonné est assurée par l'algorithme A3 (figure I-7) qui exige que le MS et l'opérateur ont la même clé K_i en calculant un code aléatoire *SRES (Signature Response)*.

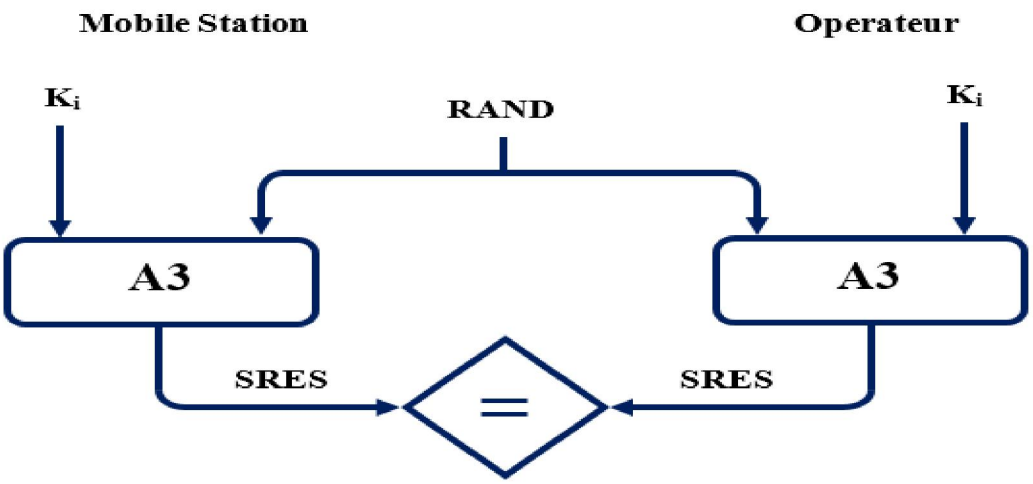


Figure I-7 : Algorithme A3

Le transfert des données via le réseau GSM est sécurisé grâce au mécanisme de cryptage A5. Le cryptage se fait uniquement entre le MS et le BTS ; ailleurs aucun cryptage n'est valable. A5 utilise une clé symétrique K_c (Cipher Key) qui est générée grâce au mécanisme A8 (figure I-8) en utilisant la clé K_i.

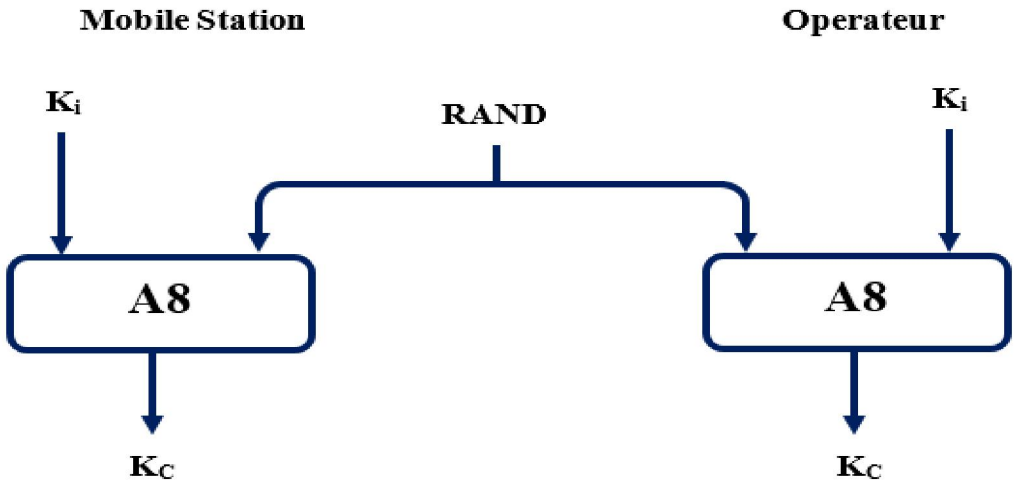


Figure I-8 : Algorithme A8

L'algorithme A5 (dit algorithme de chiffrement à flot) utilise la clé Kc et les données comme paramètres pour générer la donnée cryptée Ekc qui sera circulée dans le réseau entre le MS et le BTS. Ekc sera aussi décryptée par le même algorithme grâce à la symétrie de la clé Kc.

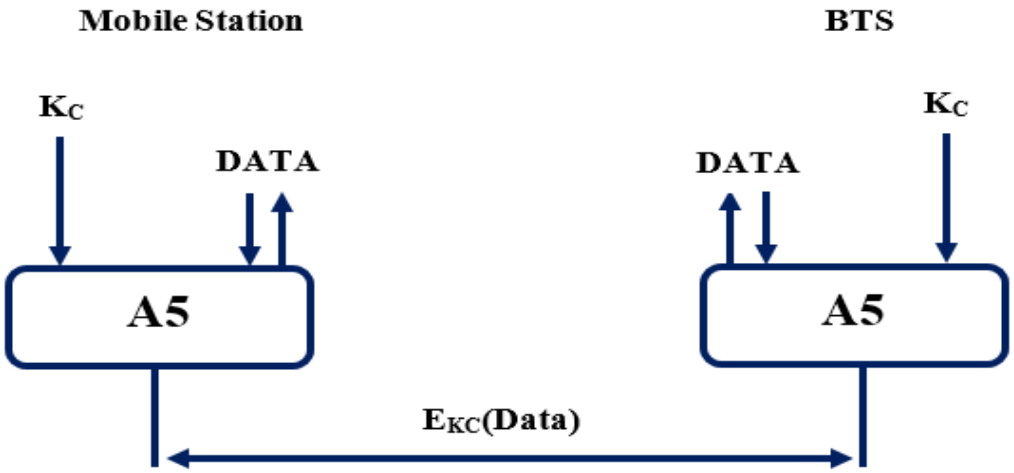


Figure I-9 : Algorithme A5

I.5. E-Banking en Algérie

Le secteur bancaire algérien a connu ces dernières années de nombreuses mutations (privatisation des banques publiques, arrivée de nouveaux acteurs issus du Moyen-Orient, de l'Europe…). A ce titre, les banques algériennes doivent aujourd'hui refondre leur système d'information afin d'accélérer leurs développements.

Dans le cadre de la modernisation de ses infrastructures et de l'amélioration constante de la qualité des prestations financières dispensées à sa clientèle les banques en Algérie ont mis en service son propre système monétique.

Ce système qui repose sur une solution monétique complète, dispose d'une interface en temps réel avec le système d'information central et permet un contrôle du solde du compte bancaire lors des transactions de retrait d'espèces sur les Distributeurs Automatiques de Billets de Banque (DAB) et les Guichets Automatiques de Banques (GAB).

I.5.1. Carte CIB (carte interbancaire)

La carte CIB, est une carte interbancaire, elle est identifiée par le logo de l'interbancarité, l'appellation, le logo de la banque émettrice.

La carte contient un microprocesseur appelé communément « puce » qui assure la sécurité dans le déroulement des transactions de paiement. [9]

Elle permet à son titulaire appelé « porteur de carte » de régler ses achats auprès de différents commerces de détail tels que les hôtels, les restaurants, les magasins superettes, les pharmacies...

C'est un instrument de paiement et de retrait interbancaire domestique qui est accepté chez les commerçants affiliés au réseau monétique interbancaire et surtout les DAB installés sur le territoire national.

Actuellement il y a deux types de carte CIB :

I.5.1.1. Carte classique

La carte classique, offrant des services de paiement et de retrait interbancaire. Elle est proposée à la clientèle selon les critères arrêtés par chaque banque.

Figure I-10 : Carte classique (Blue)

I.5.1.2. Carte Gold

La carte gold, proposée également à la clientèle selon les critères arrêtés ; Outre le paiement et le retrait d'espèces, cette carte offre des fonctionnalités supplémentaires et des plafonds de retrait et de paiement plus important.

Figure I-11 : Carte Gold

Le client peut faire des retraits et des virements utilisant ces cartes. [9]

I.5.2. Internet-Banking en Algérie

Comme exemple en prend le site d'Algérie poste ; après avoir le code secret, le client peut consulter son compte en visitant le lien suivant : eccp.poste.dz, le client peut consulter son compte, commander des chéquiers, voir l'historique de compte, demande de carte à puce… [10]

Il existe d'autre banque qui offre ce service comme : Société générale, BADR, BNA, CNEP,…

I.5.3. SMS Banking en Algérie

L'opérateur MOBILIS a lancé un service de SMS-Banking appelé (RACIDI), ce service permet de consulter en exclusivité le solde CCP à tout moment, par un simple envoi d'un SMS. Pour connaître son solde CCP, le client envoie par SMS au 603 le numéro de son CCP (sans la clé) suivi d'un espace et du code confidentiel.

En réponse le client reçoit instantanément un SMS contenant :

- Le numéro de CCP.
- Le montant de solde.
- La date de la dernière mis à jour. [11]

I.6. Conclusion

L'explosion du nombre de terminaux mobiles dans le monde, au point de dépasser celui des ordinateurs, est un fait économique important. Avec les nouveaux réseaux de télécommunication et l'accroissement des capacités de traitement des terminaux, de nouvelles possibilités d'interagir et de communiquer avec les clients, y compris via le réseau Internet, ont fait leur apparition. Ainsi, l'Internet Mobile apporte des opportunités d'élargissement de la palette des services proposés par les banques.

L'amélioration de ces techniques électroniques du système bancaire a pour but de faire face aux défis de l'ère moderne, et assure la circulation des services bancaires avec une grande efficacité.

Dans ce chapitre, nous avons présenté l'architecture du réseau GSM, qui est le moyen de communication entre le client et la banque. Nous avons présenté aussi des généralités sur l'E-Banking.

Dans le chapitre suivant nous allons présenter le réseau internet et les protocoles utilisés.

Chapitre II L'accès Internet

II.1. Introduction

L'accès à Internet est souvent vendu sous la forme d'offre commerciale de services, avec un abonnement fixe ou un paiement aux données consommées.

Pour accéder à Internet il faut disposer d'un équipement IP ainsi qu'une connexion à un fournisseur d'accès. Pour cela, l'utilisateur emploie des matériels et logiciels tel que (ordinateur, Téléphone mobile, navigateur web,…).

II.2. L'Internet

Internet, réseau des réseaux, trouve son origine en 1969 avec la création du réseau militaire américain ARPANET (Advanced Research Projects Agency Network).

Le modèle ARPANET était donc sensiblement différent : au lieu de baser toute l'information sur un unique ordinateur, celle-ci est distribuée sur divers pôles géographiques, chaque pôle étant autonome. Ainsi, même si une partie de l'information se trouvait détruit, le reste pouvait toujours être exploité.

Dans les années 70, l'infrastructure d'Arpanet est mise à disposition des universités américaines. Ainsi le nombre d'utilisateurs s'élève petit à petit. Bien naturellement, Arpanet se détache petit à petit de sa vocation initiale.

Le protocole de transport TCP/IP (Transmission Control Protocol/Internet Protocol) s'impose comme protocole de communication standard sur Internet. Dès le début des années 80, ARPANET explose en deux réseaux distincts : NSFNet (National Science Foundation Network) et MILNET (le réseau militaire).

En 1980, quelques centaines de serveurs (délivrant de l'information) sont interconnectés.

En 1986, il y en a plus de 2000. Le nombre d'usagers ne cesse d'augmenter. Dans les autres pays (par exemple le Canada) des réseaux de nature équivalente (basés sur TCP/IP) émergent, pour finalement se regrouper au début des années 90. Et là, tout s'accélère !

En 1992 : le CERN (Centre Européen de Recherche Nucléaire) propose le projet World Wide Web, fournissant ainsi l'aspect convivial que tout le monde connaît (utilisation de navigateurs, ...). Dès lors, il n'est plus nécessaire d'être un initié à l'informatique. Petit à petit, les particuliers réclame le droit de s'y connecter (et de proposer de l'information). La machine est lancée.

En 2000 : on peut considérer qu'Internet n'est encore qu'un embryon. Toujours plus de personnes et de foyers rejoignent le réseau, et l'on commence à parler de visioconférence sur Internet, de commerce électronique, ... Et certain voient en Internet le successeur à la télévision,

à la téléphonie. Aujourd'hui le plus important est l'Internet mobile avec l'avènement de l'UMTS et les réseaux sans fils. [12]

II.3. Les Protocoles de communication réseau

II.3.1. Le protocole HTTP

Le protocole HTTP (Hyper Text Transfert Protocol) est le protocole le plus utilisé sur internet depuis 1990. Le but du protocole HTTP est de permettre un transfert de fichiers (essentiellement au format HTML) localisés grâce à une chaîne de caractères appelée URL entre un navigateur (le client) et un serveur Web (appelé d'ailleurs httpd sur les machines UNIX).

II.3.2. Le protocole HTTPS

La sécurité des informations transmises par HTTPS est basée sur l'utilisation d'un algorithme de chiffrement, et sur la reconnaissance de validité du certificat d'authentification du site visité.

L'HyperText Transfer Protocol Secure permet au visiteur de vérifier l'identité du site auquel il accède grâce à un certificat d'authentification émis par une autorité tierce réputée fiable. Il garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur. Il peut permettre de valider l'identité du visiteur si celui-ci utilise également un certificat d'authentification client.

HTTPS est généralement utilisé pour les transactions financières en ligne : commerce électronique, banque en ligne, courtage en ligne, etc. Il est aussi utilisé pour la consultation de données privées, comme les courriers électroniques.

Depuis le début des années 2010, le HTTPS s'est également généralisé sur les Réseaux sociaux, la figure suivante illustre une présentation HTTPS. [13] , [14]

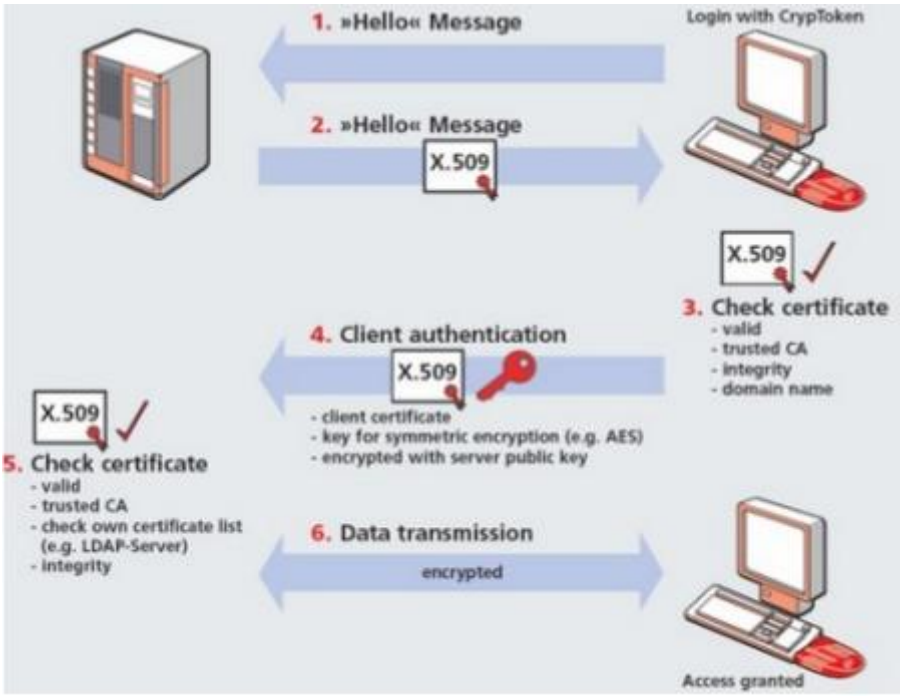


Figure II-1: Présentation HTTPS

II.3.3. TLS (Transport Layer Security)

Transport Layer Security (TLS), et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet, développés à l'origine par Netscape (SSL version 2 et SSL version 3). Il a été renommé en Transport Layer Security (TLS) par l'IETF (Internet Engineering Task Force « Détachement d'ingénierie d'Internet ») à la suite du rachat du brevet de Netscape par l'IETF en 2001. [15]

TLS a tout de même mis en place un mécanisme de compatibilité ascendante avec SSL. En outre, TLS diffère de SSL pour la génération des clés symétriques. Cette génération est plus sécurisée dans TLS que dans SSL version 3 dans la mesure où aucune étape de l'algorithme ne repose uniquement sur MD5 pour lequel sont apparues des faiblesses en cryptanalyse.

Le protocole TLS permet de créer un tunnel entre un ordinateur et un serveur. Ce tunnel sécurisé permet un échange d'informations en contournant les dispositifs de sécurité installés pour un serveur ou un ordinateur. Passant outre les systèmes de protection il est alors possible que des actions malveillantes soient menées au travers du point d'entrée du tunnel. Afin de limiter les risques, il est techniquement possible de filtrer les contenus d'un tunnel TLS par la mise en place d'un dispositif qui authentifie le client et le serveur. Deux tunnels sont alors mis en place, un depuis le client vers le dispositif d'authentification et le second du dispositif vers le serveur. Ce système permet alors une analyse et une sécurisation transparente des contenus transférés par le tunnel TLS comme il est montré dans la figure suivante :

Figure II-2 : Protocole TLS

II.3.4. Authentification du client SSL par certificat numérique

L'utilisateur authentifie le serveur TLS sur lequel il se connecte. Cette authentification est réalisée par l'utilisation d'un certificat numérique X.509 délivré par une autorité de certification (AC). Mais de plus en plus d'applications web utilisent maintenant l'authentification du poste client en exploitant TLS. Il est alors possible d'offrir une authentification mutuelle entre le client et le serveur. Le certificat client peut être stocké au format logiciel sur le poste client ou au format matériel (carte à puce, USB) pour augmenter la sécurité du lien TLS. Cette solution permet d'offrir des mécanismes d'authentification forte.(15)

II.3.5. FTP

Le protocole FTP (File Transfer Protocol) est, comme son nom l'indique, un protocole de transfert de fichier.

Il est actuellement défini par le RFC 959 (File Transfer Protocol (FTP) - Spécifications). Le protocole FTP définit la façon selon laquelle des données doivent être transférées sur un réseau TCP/IP. [12]

II.3.6. URL

Une URL (Uniform Resource Locator) est un format de nom universel pour désigner une ressource sur Internet. Il s'agit d'une chaîne de caractères ASCII imprimables qui se décompose en cinq parties comme elle est structurée dans la figure II-3 : Le nom du protocole, Identifiant et mot de passe, Le nom du serveur, Le numéro de port, Le chemin d'accès à la ressource.

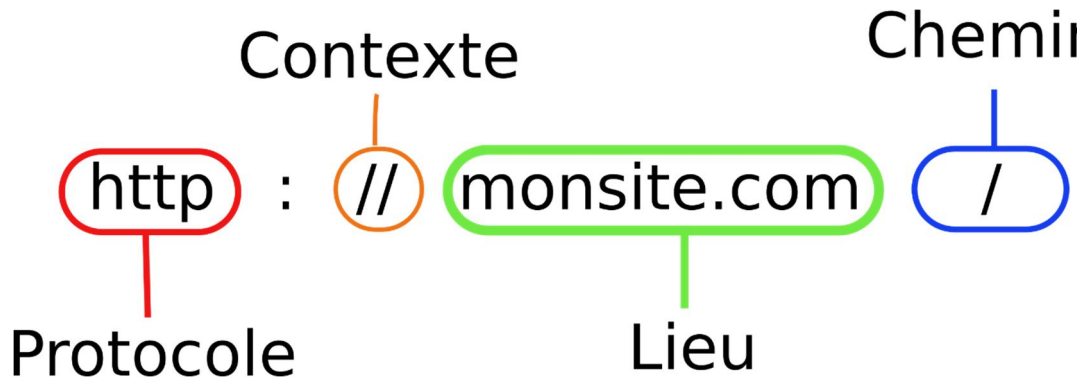


Figure II-3 : Structure d'une URL

II.3.7. Site Web

Un site Web (aussi appelé site Internet ou page perso dans le cas d'un site Internet à but personnel) est un ensemble de fichiers HTML stockés sur un ordinateur connecté en permanence à Internet et hébergeant les pages Web (serveur Web).

Un site Web est habituellement architecturé autour d'une page centrale, appelée «page d'accueil» et proposant des liens vers un ensemble d'autres pages hébergées sur le même serveur, et parfois des liens dits «externes», c'est-à-dire de pages hébergées par un autre serveur.

II.4. Cryptographie

Si le but traditionnel de la cryptographie est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle, la cryptographie moderne s'attaque en fait plus généralement aux problèmes de sécurité des communications. Le but est d'offrir un certain nombre de services de sécurité comme la confidentialité, l'intégrité, l'authentification des données transmises et l'authentification d'un tiers. Pour cela, on utilise un certain nombre de mécanismes basés sur des algorithmes cryptographiques. [16]

II.4.1. Chiffrement symétrique ou à clef secrète

Dans la cryptographie conventionnelle, les clefs de chiffrement et de déchiffrement sont identiques : c'est la clef secrète, qui doit être connue des tiers communiquant et d'eux seuls. Le procédé de chiffrement est dit symétrique.

Les algorithmes symétriques sont de deux types :

- Les algorithmes de chiffrement en continu, qui agissent sur le texte en clair un bit à la fois.

- Les algorithmes de chiffrement par blocs, qui opèrent sur le texte en clair par groupes de bits appelés blocs.

II.4.2. Chiffrement asymétrique ou à clef publique

Avec les algorithmes asymétriques, les clefs de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire l'une de l'autre. On peut donc rendre l'une des deux publique tandis que l'autre reste privée. C'est pourquoi on parle de chiffrement à clef publique. Si la clef publique sert au chiffrement, tout le monde peut chiffrer un message, que seul le propriétaire de la clef privée pourra déchiffrer. On assure ainsi la confidentialité. Certains algorithmes permettent d'utiliser la clef privée pour chiffrer. Dans ce cas, n'importe qui pourra déchiffrer, mais seul le possesseur de la clef privée peut chiffrer. Cela permet donc la signature de messages.

II.4.3. Fonctions de hachage à sens unique

Aussi appelée fonction de condensation, une fonction de hachage est une fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe ; la chaîne résultante est appelée empreinte (digest en anglais) ou condensé de la chaîne initiale.

Une fonction à sens unique est une fonction facile à calculer mais difficile à inverser. La cryptographie à clef publique repose sur l'utilisation de fonctions à sens unique à brèche secrète : pour qui connaît le secret (i.e. la clef privée), la fonction devient facile à inverser.

II.4.3.1. MD5 (Message Digest 5)

Développé par Rivest en 1991, MD5 produit une empreinte de 128 bits à partir d'un texte de taille arbitraire. MD5 manipule le texte d'entrée par blocs de 512 bits.

II.4.3.2. SHA (Secure Hash Algorithm)

SHA est la fonction de hachage utilisée par SHS (Secure Hash Standard), la norme du gouvernement Américain pour le hachage. SHA-1 est une amélioration de SHA publiée en 1994. SHA-1 produit une empreinte de 160 bits à partir d'un message de longueur maximale 2^{64} bits. Tout comme MD5, SHA-1 travaille sur des blocs de 512 bits.

II.4.4. Signature numérique

La norme [ISO 7498-2] définit la signature numérique comme des "données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à

un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire par exemple)". La mention « protégeant contre la contrefaçon » implique que seul l'expéditeur doit être capable de générer la signature comme représenté dans la figure suivante :

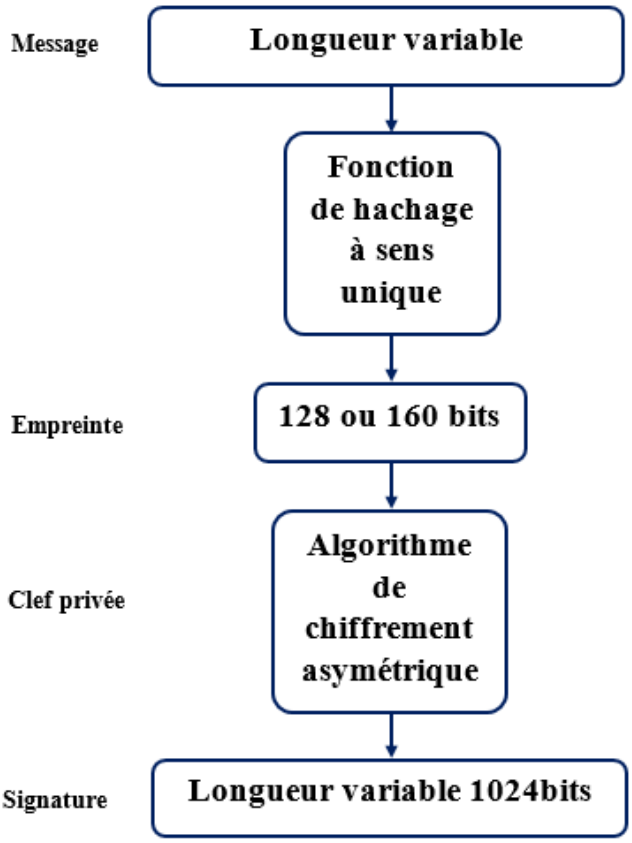


Figure II-4 : Signature.

II.5. Le TCP/IP

Internet est constitué de tous les réseaux utilisant le même protocole de communication : TCP/IP. Protocole créé en 1974 par Vinton Cerf et Robert Kahn, et mis dans le domaine public par le Pentagone en 1983.

C'est la diffusion libre et gratuite de TCP/IP qui a permis le développement de l'Internet.

TCP/IP permet l'interconnexion de réseaux hétérogènes (réseaux de grande distance, MAN, réseaux locaux...), utilisant eux-mêmes différents protocoles spécifiques (Ethernet...). Il repose notamment sur un système d'adresses, les adresses IP sont attribuées à chaque machine.

La figure suivante représente l'architecture de protocole TCP/IP. [14]

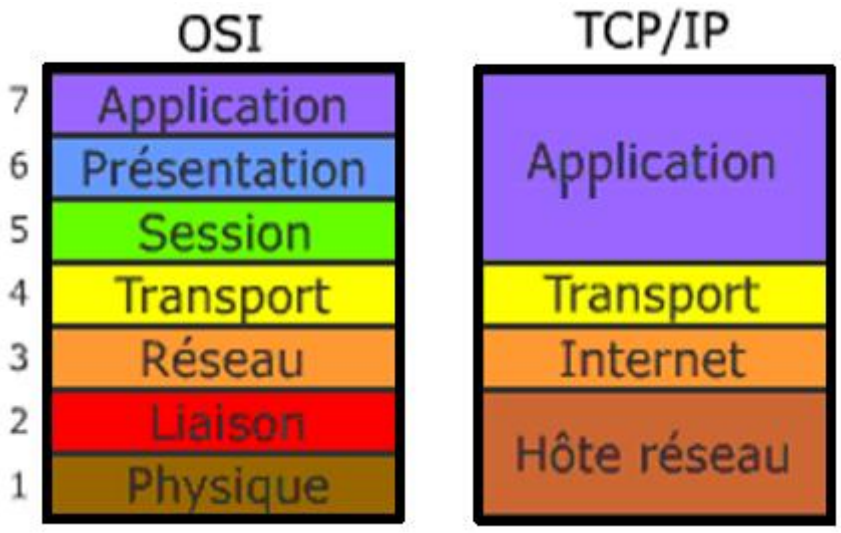


Figure II-5 : Architecture de TCP/ IP.

Couche Accès (Hôte réseau)

La couche Accès correspond en gros aux couches (1 et 2) de modèle OSI. N'importe quel réseau physique peut être a priori utilisé pour transporter le protocole TCP/IP il suffit qu'il existe un standard RFC (Request For Comment) et qu'un « driver » soit disponible.

Les réseaux les plus souvent utilisés sont bien sûr les réseaux locaux (Token-Ring, Ethernet, FDDI), mais on peut aussi s'appuyer sur un transport X25, SNA ou Net BIOS, des liaisons asynchrones (SLIP), etc…

Couche Internet (IP)

La couche IP correspond au 3ème niveau de modèle OSI (réseau de routage). On envoie un datagramme et on « espère » qu'il arrive. Les contrôles d'erreur, contrôles de flux, remise en ordre des datagrammes, sont donc à la charge des couches supérieures.

Couche Transport Hôte à Hôte (TCP)

La couche TCP correspond à la couche 4eme couche de modèle OSI (transport de bout en bout) et assure également le multiplexage des connexions IP vers les applications (Connected Less and Oriented). On peut aussi utiliser UDP qui ne fait que ce multiplexage et laisse aux couches supérieures les différents contrôles.

Couche Application

Enfin, la couche application (équivalente aux couches 5, 6 et 7 de modèle OSI), comporte un certain nombre d'applications standardisées qui s'appuient elles-mêmes sur TCP ou UDP.

Elle comprend l'émulation de terminal (TELNET), le transfert de fichiers (FTP) et la messagerie (SMTP). Chaque couche de la pile ajoute des informations de contrôle de manière à garantir une transmission de données correcte.

II.6. L'IP Mobile

Défini par l'IETF, Mobile IP propose une solution pour résoudre le problème de changement de point d'attachement à l'Internet. Mobile IP maintient la même adresse IP quelle que soit la localisation du terminal, de telle façon qu'il ait en permanence un identifiant unique. Le nouveau protocole a la responsabilité de transmettre les paquets au terminal quelle que soit la manière dont il se déplace dans le réseau et d'indiquer de façon signifiante le point de localisation.

Mobile IP permet uniquement d'introduire de la mobilité dans les réseaux IP. Les réseaux cellulaires, avec leurs propres mécanismes internes de gestion de la mobilité, permettent au nœud mobile de garder la connectivité avec un point d'attachement Internet unique (NAS pour un accès circuit, GGSN pour un accès paquet). Le protocole Mobile IP ne s'impose donc pas nécessairement dans les réseaux cellulaires. Par contre, il peut être utilisé de manière efficace en "overlay" afin de permettre la mobilité entre réseaux de natures différentes.

Mobile IP permet à un mobile disposant de plusieurs interfaces radios de passer indifféremment d'un réseau cellulaire public (GSM/GPRS/UMTS) à un réseau privé d'entreprise sans fil (WLAN). Par contre il ne supporte pas pour l'instant une mobilité rapide entre cellules radio de type WLAN : le temps de latence lors du handover n'est pas optimisé (manque d'échange d'informations de contrôles entre la couche liaison et la couche IP, délai de mise à jour de la nouvelle localisation vers le réseau mère qui peut être très éloigné du point d'attachement courant). Les groupes de travail de l'IETF prévoient les améliorations nécessaires mais, tant qu'elles ne sont pas spécifiées, il n'est pas envisageable de supporter "sans coupure" des services à fortes contraintes temps réel tels que la téléphonie ou la vidéo sur IP. [12]

II.7. L'Internet mobile

Les utilisateurs de mobiles demandent à accéder aux ressources d'informations via leurs mobiles. Il est impossible pour les opérateurs d'ignorer ce besoin d'intégration de systèmes mobiles avec l'environnement Internet.

Le réseau numérique de Packet-Switched résout une partie du problème d'accès à l'Internet sans fil. Les opérateurs des réseaux mobiles ont besoin de trouver une façon pour fournir au client le service d'accès au réseau extérieur rapidement et moins cher.

Mais il y a un obstacle sur l'intégration de réseau mobile avec le réseau Internet : les protocoles adoptés par le réseau numérique et mobile n'existent pas en dehors de ce système.

Les protocoles Internet sont des standards de facto de communication sur le réseau filaire. Ils constituent des points communs pour cette intégration. Les opérateurs du réseau mobile peuvent fournir un service d'accès à l'Internet soit par intégration des protocoles Internet en haut de ceux existant sur le réseau mobile, soit en établissant un Gateway propriétaire entre l'Internet et les machines mobiles qui supportent GUI (Graphical User Interfaces) en base de la technologie Internet**.** Cela peut permettre aux utilisateurs la connexion avec des opérateurs du réseau mobile ou avec tous les sites d'information sur Internet.

En effet, beaucoup de porteurs du réseau mobile ont déjà commencé à mettre en état des protocoles Internet comme base des échanges des informations entre des appareils mobiles et le réseau externe. Par exemple, M_Banking.

Pour le moment, les applications pour les réseaux 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 séparer les applications pour les réseaux sans fil et les réseaux de mobiles.

II.7.1. Le contrôle de l'Internet mobile

L'Internet mobile comme l'Internet fixe doit être contrôlé. De nombreuses solutions sont utilisées par l'intermédiaire des systèmes de signalisation des différents réseaux composant l'Internet mobile. D'une manière générale, un système de gestion comme SNMP (Simple Network Management Protocol) est capable de réaliser un contrôle du réseau qu'il gère. Mais SNMP est un protocole lourd et qui réagit lentement.

II.7.2. La sécurité dans l'Internet mobile

Comme tous les réseaux, la sécurité est un problème pour l'Internet mobile. La mobilité la complique encore puisque l'utilisation d'une interface radio permet à un tiers d'écouter la porteuse et de recopier ce qui est transporté.

La sécurité de l'Internet mobile reprend la plupart des protocoles qui sont définis pour le fixe et qui comportent deux grande catégories : les protocoles qui assurent au moment de la mise en place de la communication, ce sont les bons processus qui communiquent et ceux qui assurent que la communication elle-même est sécurisée par un chiffrement.

II.7.3. La gestion de la mobilité

La gestion de la mobilité désigne la possibilité de continuer la communication dans les

meilleures conditions possibles, même lors d'un déplacement du terminal. Classiquement, la gestion de la mobilité s'effectue par l'intermédiaire d'un agent home (home agent) qui détient les caractéristiques de l'utilisateur, et d'un agent visité (forgien agent), qui gère le client localement. Dans l'environnement de l'Internet mobile, ou les cellules peuvent devenir toutes petites, il n'est plus convenable qu'à chaque changement de cellule l'agent visité avertisse l'agent home au risque de surcharger de façon démesurée le réseau. Il faut donc cacher a l'agent home que le terminal bouge.

Il y a aussi IP Mobile qui permet de gérer la mobilité mais en passant par l'agent home et que cette technique ne s'applique qu'à des déplacements lents ou à des changements de lieu de terminal.

II.8. WAP (Wireless Application Protocol)

La technologie WAP a pour but de permettre à des terminaux mobiles (les téléphones portables par exemple) d'accéder à des documents circulant par des réseaux sans fil. Il s'agit donc de permettre à n'importe quel terminal mobile de pouvoir formater des documents. C'est pour cela qu'un protocole universel a été mis en place.

Le WAP (**Wireless Application Protocol** ou en français Protocole d'Application Mobile). Il se propose de définir la façon de laquelle les terminaux mobiles accèdent à des services Internet, et cela à un niveau au-dessus de la transmission des données, celle-ci étant spécifique à chaque opérateur de téléphonie. [17]

Le WAP est né de l'alliance en 1997 de plusieurs grands groupes regroupant des constructeurs de mobiles (**Nokia, Ericsson...**), des opérateurs en téléphonie mobile et des multinationales (**Phone.com, Microsoft..**.) au sein du WAP Forum.

Celui-ci est chargé de valider les spécifications techniques proposées par les sociétés participantes. La version 1.0 du protocole WAP a été publiée en Mai 1998.

Les spécifications du WAP sont libres, c'est à dire que quiconque peut les lire et en apprendre le fonctionnement.

L'ensemble des protocoles WAP ont été développés dans le respect des protocoles multicouches du modèle OSI, si bien que l'on peut faire un parallèle entre la pile TCP/IP et le WAP (figure II-6).

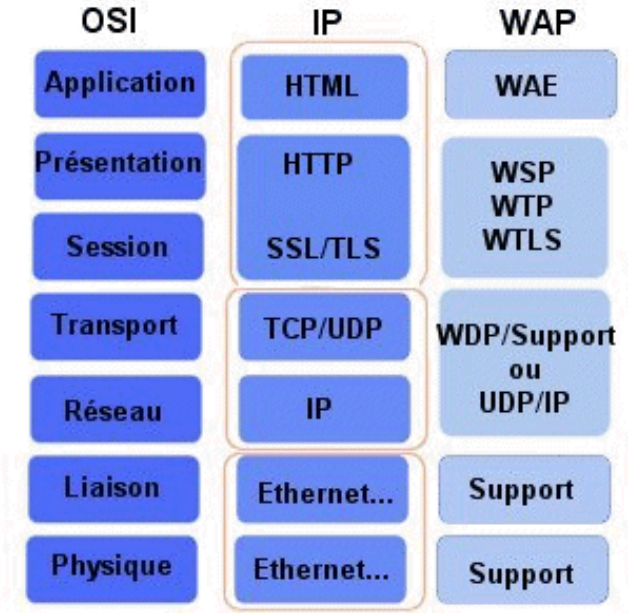


Figure II-6 : la pile TCP/IP et le WAP

II.8.1. Structure de la pile protocolaire

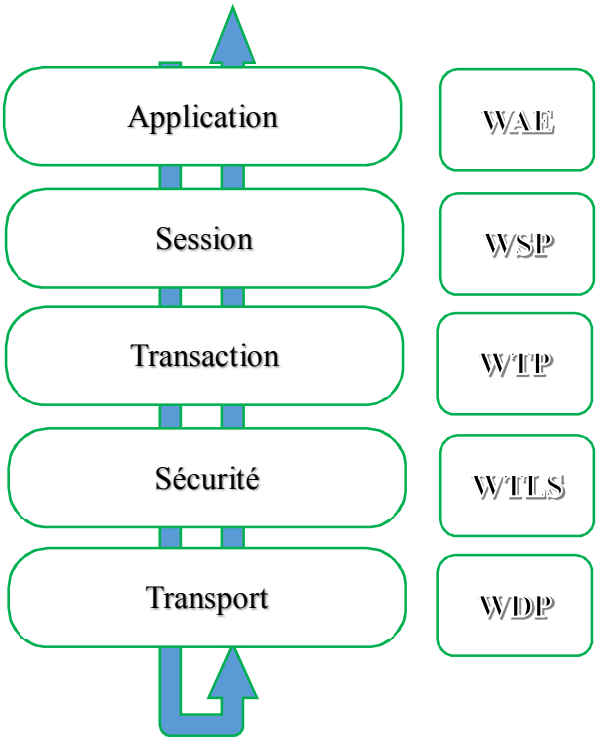


Figure II-7 : La pile protocolaire du WAP

II.8.1.1. WAE (Wireless Application Environnent)

La couche application se situe au niveau le plus haut de la pile WAP. Elle a pour but d'offrir une connectivité grâce à laquelle les contraintes entre opérateurs téléphoniques, fournisseurs et constructeurs de terminaux disparaissent. Cette couche est un mélange de différentes techniques issues du Web et de la téléphonie. C'est la couche application qui définit l'interface utilisateur sur son mobile et que des applications peuvent être développées. Cette couche intègre les spécificités du WML, du WMLScript et du WTA (Wireless Telephony Application) : ensemble d'interfaces permettant d'accéder à différentes fonctions de téléphonie d'un terminal comme exemple la composition d'un numéro).

II.8.1.2. WSP (Wireless Session Protocol)

La couche session est constituée de deux protocoles :

Les protocoles orientés connexion : Il s'agit des protocoles opérant un contrôle de transmission des données pendant une communication établie entre deux machines.

Dans un tel schéma, la machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données qu'elle envoie. Les données sont ainsi envoyées sous forme de flot. Exemple : TCP est un protocole orienté connexion.

Les protocoles non orientés connexion : Il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première. Les données sont ainsi envoyées sous forme de blocs (datagrammes). Exemple : UDP est un protocole non orienté connexion.

II.8.1.3. WTP (Wireless Transaction Protocol)

La couche de transaction gère le déroulement de la transaction, elle définit donc la fiabilité du service. La communication peut se faire de trois façons :

- à sens unique avec acquittement
- à sens unique sans acquittement
- en full duplex avec acquittement

Elle permet en outre d'effectuer des transactions synchrones et de retarder les acquittements afin de les gérer par paquets.

II.8.1.4. WTLS (Wireless Transport Layer Secure)

Puisque les données circulent entre le terminal mobile et la passerelle grâce à des réseaux sans fil, il est nécessaire que les transactions soient sécurisées, c'est ce que se propose de faire la couche sécurité. Celle-ci est basée sur le standard SSL (Secure Socket Layer) et permet :

- de crypter les échanges de données
- de garantir l'intégrité des données (vérifier que celles-ci n'ont pas été modifiées)
- d'authentifier les acteurs de l'échange

II.8.1.5. WDP (Wireless Datagram Protocol)

La couche WDP est à la base de la pile de protocoles WAP, c'est elle qui est chargée de l'interface avec les protocoles de transmission de données utilisés par les opérateurs de télécoms :

- GSM data
- HSCSD
- GPRS
- UMTS

II.8.1.6. Un exemple de réseau WAP

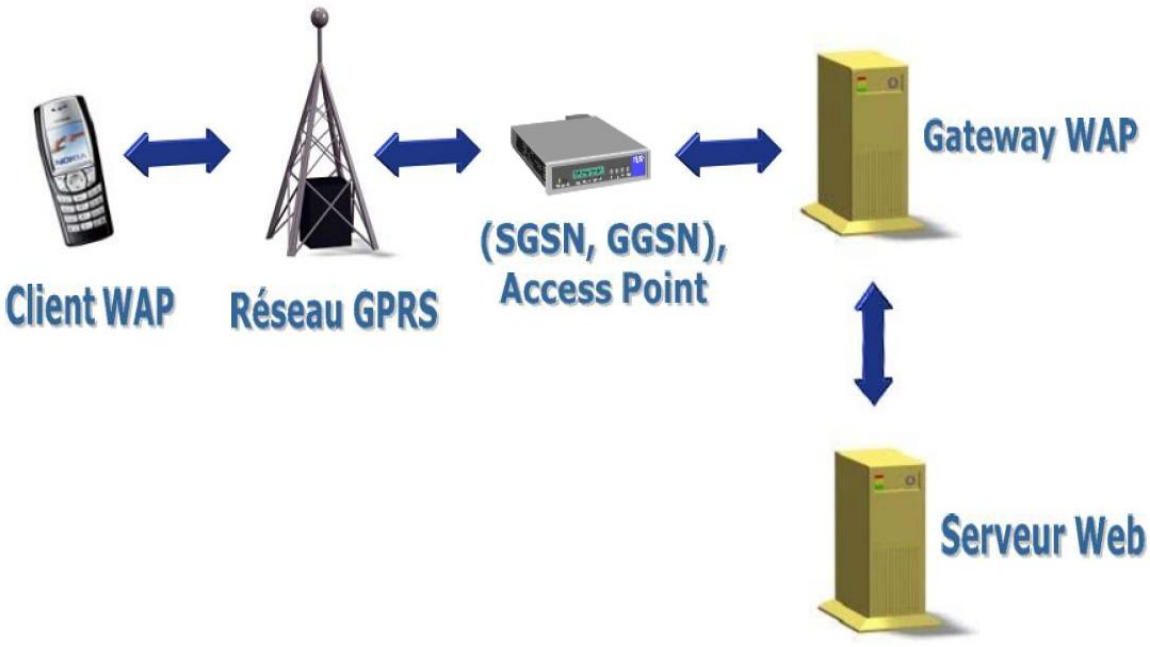


Figure II-8 : Exemple d'un réseau WAP.

II.8.2. Les passerelles

D'un point de vue architecture, le terminal communique avec le serveur d'information par l'intermédiaire d'une passerelle. Cette passerelle adapte les mondes GSM par exemple et Internet en convertissant les protocoles de transport WAP s'il s'agit d'un téléphone cellulaire de ce standard en protocole Internet classique (HTTP). Elle assure également les fonctions d'authentification, de sécurité, de facturation, de gestion des profils utilisateurs, etc.

Certaines de ces fonctions pouvant être localisées au niveau de la plate-forme ISP (Internet Service Provider).

II.8.2.1. Passerelle chez un fournisseur

Cette solution présente l'avantage, pour les fournisseurs d'accès, de ne pas être dépendants des opérateurs téléphoniques et de pouvoir ainsi administrer leur propre passerelle WAP. Dans ce cas, seule la connectivité GSM/RTC des opérateurs est utilisée.

L'utilisateur compose ainsi directement le numéro du fournisseur qui devient donc un opérateur téléphonique alternatif spécialisé dans la connexion Internet via le WAP.

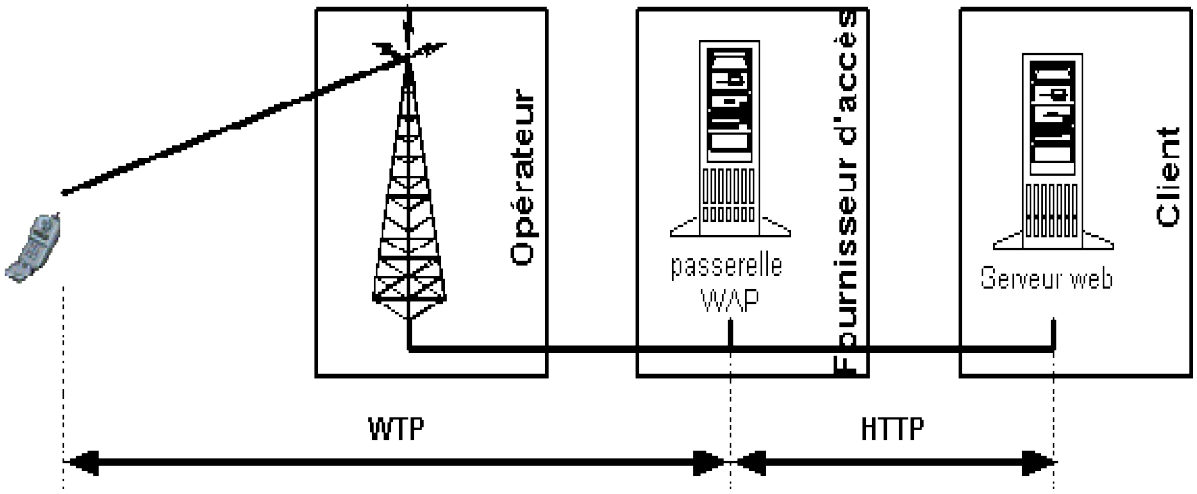


Figure II-9 : Passerelle WAP chez le fournisseur

II.8.2.2. Passerelle WAP en interne

Si le client veut garder la maîtrise complète des connexions WAP, il peut décider d'avoir sa propre passerelle WAP, on se retrouve alors dans la situation ci-dessous

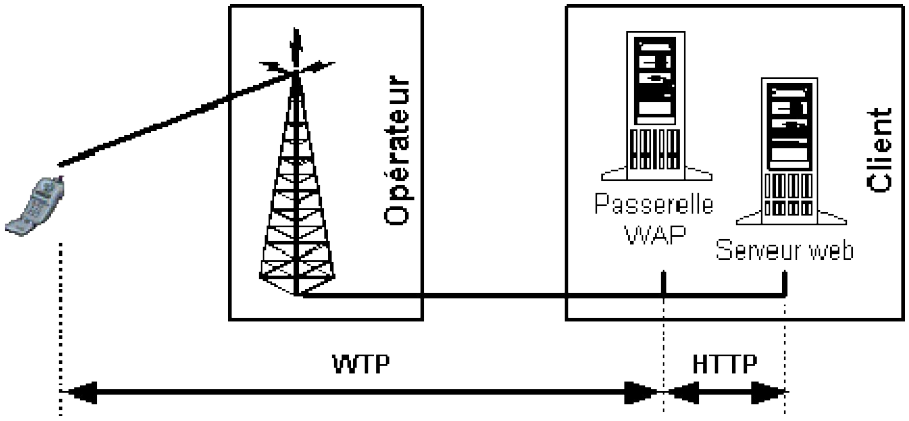


Figure II-10 : Passerelle WAP interne

Cette solution peut être envisageable dans le cas d'applications WAP dédiées à une entreprise et exploitant des données sur l'Intranet.

II.9. WIFI (Wireless Fidelity)

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. [13]

II.10. Conclusion

Aujourd'hui Internet, lieu où se côtoient conviviale ment chercheurs, enseignants, étudiants, sociétés commerciales et tant d'autre semble être en pleine mutation. Personne actuellement ne peut dire à quoi ressemblera Internet dans les années à venir. Mais l'arrivée d'entreprises commerciales sera l'un des facteurs clés de l'avenir, le " net " risque de devenir à plus ou moins longs terme, un réseau payant. Ce qui est contraire pour le moment aux règles du réseau.

L'évolution des terminaux se fait en parallèle avec celle des services fournis par les réseaux mobiles car on ne peut pas accéder à un service donné sans avoir le terminal adéquat.

L'accès à l'Internet mobile se fait avec différents protocoles, et applications fourni par les opérateurs des différents pays.

Chapitre III Langages et logiciels utilisés

III.1. Introduction

Disposant de plusieurs techniques et technologies pour mettre en œuvre notre plateforme, il a fallu au préalable que nous choisissons celles avec lesquelles nous allons implémenter la solution en tenant compte des contraintes informatiques et techniques : langage, base de données, matériel… etc.

Ce chapitre mis le point sur les différents outils et langages que nous avons utilisé pour développer les différentes interfaces de nos applications.

III.2. Mise en place d'un serveur de développement

Les critères, sur lesquels nous sommes basés pour choisir les outils de développement de la plateforme, nous ont amené à choisir des langages de développement interprétés (des langages de script) interfacés avec un système de gestion de bases de données.

III.2.1. Le serveur Web APACHE

Le serveur que nous avons utilisé est de type Apache. Il s'agit d'un système de serveur libre et open-source développé par The Apache Software Fondation avec Microsoft IIS, il est le serveur web le plus utilisé. Sa gratuité, le dynamisme de sa communauté, son coût réduit en fait l'un des systèmes de choix pour les petits et moyens projets. [18]

Apache est une application fonctionnant sous les systèmes d'exploitation de la famille UNIX, mais il a désormais été porté sur différents autres systèmes dont Windows, il possède désormais de nombreuses fonctionnalités dont la possibilité de définir une configuration pour chaque fichier ou répertoire partagé ainsi que les restrictions sur les droits d'accès. Il est associé au langage de scripte PHP que nous utiliserons pour l'implémentation de notre plateforme. [19]

Apache peut héberger des sites Web statiques, ainsi que des sites Web dynamiques qui utilisent des langages de script côté serveur, tels que PHP, Perl ou Python. Support pour ces et d'autres langues a été ajouté par le biais de modules ou les packages d'installation qui sont ajoutés à l'installation standard d'Apache. Apache supporte aussi les autres modules, qui offrent des options de sécurité avancées, outils de gestion de fichiers et d'autres fonctionnalités. La plupart des installations d'Apache incluent un module de réécriture URL appelé « mod_rewrite », qui est devenu un moyen courant pour les webmasters créer des URL personnalisées.

III.2.2. Le langage interprété PHP

Initialement appelé Personal Home Page, il a été développé à l'origine par Rasmus Lerdorf en 1994 pour enregistrer le nombre de visiteurs sur son site. Il a vite été perfectionné par la communauté internet pour devenir un langage de script côté serveur. PHP est libre, portable et facile à comprendre. [20]

III.2.2.1. Fonctionnement

Le noyau PHP est un moteur en langage « C » localisé sur le serveur. Quand un fichier est appelé par un navigateur web, selon son extension (.htm, .php, .asp…), le serveur l'envoie directement au navigateur pour qu'il affiche la page ou le traite (dans le cas d'un fichier .php) en exécutant les commandes du langage PHP dont le résultat est renvoyé sous forme de code HTML.

III.2.2.2. Utilisation du formulaire

L'un des points forts de PHP est sa capacité à gérer les formulaires. Le concept de base qui est important à comprendre est que tous les champs d'un formulaire seront automatiquement disponibles dans le script PHP d'action.

La création d'un formulaire nécessite la connaissance de quelques balises HTML indispensables. Un formulaire commence toujours par la balise <form> et se termine par la balise </form> entre ces deux balise se situent les balise qui créeront les différent types de champs que contiendra le formulaire.

III.2.2.3. Méthode d'envoi GET et POST

Dans la définition de l'attribut « method » dans la balise <form> on a le choix entre les valeurs GET ou POST pour l'envoi des données. La méthode GET ajoute les noms des variables et leur valeur dans l'URL. Elle a pour inconvénient de rendre visible les données dans la barre d'adresse du navigateur, de plus, la langueur totale est limitée à 255 caractères, ce qui rend impossible la transmission d'un volume de données important. Cette méthode est désormais considérée comme « dépréciée » par la recommandation sur le HTML 4.0 du W3C (Word Wide Web Consortium). On lui préféra donc la méthode POST, avec laquelle le volume des données n'est pas limité et qui présente une plus grande garantie de confidentialité des données.

III.2.2.4. Récupération des données dans PHP

Lors de la soumission du formulaire, PHP crée autant de variables globales qu'il y a des champs nommés dans le formulaire et leur attribue comme nom la valeur de l'attribut HTML “name“ défini pour chaque champ et comme valeur, la valeur de l'attribut HTML “value“. Le scripte PHP désigné dans l'attribut “action“ recevra ces noms de variable et leur valeur pour leur appliquer un traitement éventuel.

III.2.3. Dynamisation des pages Web coté client : Javascript

JavaScript est un langage de script orienté objet principalement utilisé dans les pages HTML. A l'opposé des langages serveurs (qui s'exécutent sur le site), JavaScript est exécuté sur l'ordinateur de l'internaute par le navigateur lui-même. Il permet de :

- Animer le bas de page en changeant le texte de la barre d'état ;
- Réaliser des contrôles de saisie localement ;
- Ouvrir de nouvelles fenêtres (popup) ;
- Réaliser des fonctions d'historique sur les pages visitées ;
- Modifier les propriétés des documents affichés (taille, contenus, couleurs, mise en forme…) ; [21]

III.2.4. Langage XHTML et CSS

Le XHTML est une évolution du HTML « Hypertext Markup Language », c’est-à-dire langage de marquage hypertexte, il permet de structurer le contenu des pages web dans différents éléments.

Cela signifie que la mise en place d’une page web (titres, paragraphes, images...) utilisera des caractères pour marquer d’une certaine façon les différentes parties du texte. Parmi ces caractères de marquage, certains correspondront à des liens vers d’autres pages web : ce sont des liens hypertexte.

Le « X» de XHTML vient de XML, soit « eXtensible Markup Language », langage plus complexe et plus strict que le HTML. C’est lui qui a inspiré la transition du HTML vers la forme plus rigoureuse qu’est le XHTML.

Quant à CSS, cela signifie « Cascading Style Sheets », ce qui se traduit en français par feuilles de style en cascade.

La feuille de style fournit la mise en forme des éléments de la page, qui auront été écrits en XHTML. Elle s'applique à une ou plusieurs pages du site.

Le terme « en cascade » indique que la mise en forme d'une page peut faire appel à plusieurs feuilles de style. Les différentes propriétés affectées à un même élément s'ajoutent alors pour lui donner sa mise en forme finale. Lorsque deux propriétés se contredisent, des règles de priorité s'appliquent et c'est généralement le dernier style défini qui est pris en compte. [22]

III.2.5. Le Système de Gestion de Bases de Données MySQL

MySQL est un véritable serveur de base de données SQL multiutilisateurs et multi-threaded. SQL est le plus populaire langage de base de données dans le monde.

SQL est un langage standardisé qui rend facile le stockage, la mise à jour et l'accès à l'information. Par exemple, nous utilisons le SQL pour récupérer des informations sur un produit ou stocker des informations client sur un site web. MySQL est suffisamment rapide et flexible pour gérer des historiques et des images. Les principaux objectifs de MySQL sont la rapidité, la robustesse et la facilité d'utilisation. [23]

III.3. J2ME

III.3.1. Présentation de J2ME

L'univers Java contient aujourd'hui trois plates-formes majeures :

- Java 2 Micro Edition (J2ME) : se destine au marché de l'informatique embarquée.
- Java 2 Standard Edition (J2SE) : désignent la plate-forme de développement historique destiné aux postes de travail. J2SE permet de créer des applications bureautiques, des développeurs. [24]

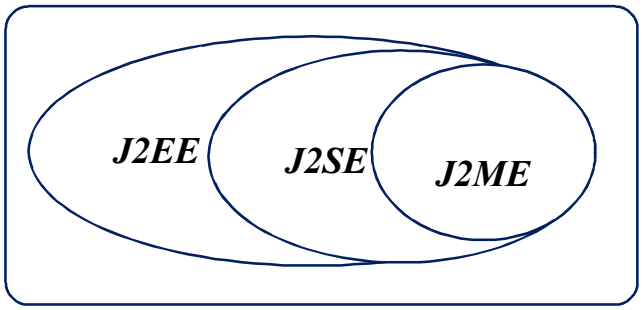


Figure III-1 : La plate-Forme Java

J2ME est un sous-ensemble de la plate-forme J2SE (Standard Edition). Elle tend à garder les qualités de la technologie Java comme :

- La portabilité du code : Les applications de Java peuvent être exécutées sur tous les systèmes d'exploitation qui possèdent une Java Virtual Machine (JVM) le programme qui interprète le byte code Java et le convertir en code exécutable.
- Un fonctionnement sur en réseau : Une gestion des applications locales et réseaux.

III.3.2. Architecture J2ME

L'architecture J2ME définit des configurations, des profils, et des paquetages facultatifs comme nous montre la figure (III-2). Elle est optimisée en fonction de la mémoire, la capacité de traitement et les possibilités d'entrées-sorties et ceci pour chaque catégorie de dispositifs. [25]

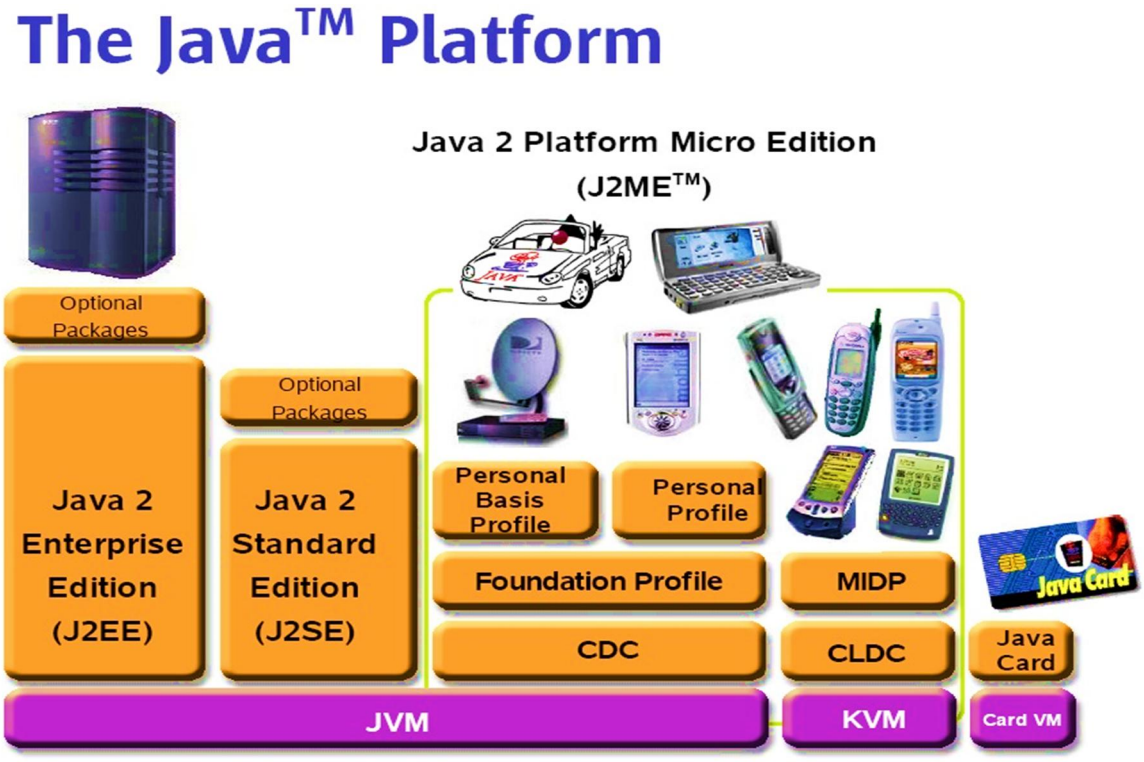


Figure III-2 : Architecture J2ME

III.3.3. Les machines virtuelles

La machine virtuelle se trouve entre l'application et la plate-forme utilisée, convertissant les bytes code de l'application en mode machine approprié au matériel et au système d'exploitation utilisé.

En fonction de la cible, la machine virtuelle pourra être allégée afin de consommer plus ou moins de ressources. J2ME propose aujourd'hui deux types de machines virtuelles : KVM (KiloByte Virtual Machine) et CVM (Convergence Virtual Machine).

III.3.3.1. KVM

Les classes Java s'exécutent dans la KVM, ont été conçues pour fonctionner dans un environnement limité en termes de mémoire (128 KB), d'énergie et d'accès réseau. Cette configuration s'inscrit donc dans une logique d'économie de ressource avec une KVM de 40 à 80 Ko s'exécutant 30 à 80 % moins vite qu'une JVM (Java Virtual Machine) normale.

III.3.3.2. CVM

La CVM a été conçue pour les terminaux ayant besoin de l'ensemble de fonctionnalités de la JVM mais avec des capacités plus réduites. Les terminaux utilisant CVM sont généralement des terminaux compacts et connectés, orientés consommateur.

III.3.4. Les profile

Lorsqu'une configuration définit le fondement d'une application, un profil en fournit la structure.

Les profiles définissent l'ensemble des API à utiliser dans une application J2ME et sont conçus spécialement pour chaque configuration.

Sun propose deux profils de référence J2ME : le profil « Foundation » et le profil « Mobile Information Device Profile » (MIDP).

III.3.4.1. Le profile Foundation

Ce profile est destiné à la configuration CDC. Les développeurs qui utilisent ce profile ont accès à une implémentation complète des fonctionnalités de J2SE.

III.3.4.2. Le profile MIDP

Ce profile est destiné à la configuration CLDC. Il prend en charge un nombre limité des classes de J2SE et définit des classes d'entrée/sortie et d'interface spécialisées pour une configuration CLDC.

III.3.5. Les Midlets

Les Midlets sont l'élément principal d'une application Java embarquée. Pour bien saisir leur mode de fonctionnement, il suffit de prendre comme analogie les applets ou les servlets.

Le cycle de vie d'une Applet est géré par un conteneur, en l'occurrence le navigateur web, dont le rôle est d'interagir avec celle-ci sous la forme de méthodes de notifications prédéfinies (init(), paint(), destryed(),…). Une servlet possède les mêmes caractéristiques qu'une Applet excepté le fait que le conteneur est un moteur de servlet (Tomcut, WebSphere, WebLogic,…).

Quant aux Midlets, ils représentent le pendant des Applets et des Servlets pour J2ME avec comme conteneur votre téléphone mobile ou votre assistant personnel. Ainsi, en cas de mise à jour d'une application embarquée, un simple téléchargement de code Midlet est nécessaire à partir d'un quelconque serveur. De cette manière, un programme développé pour un profile donné est en mesure de s'exécuter sur tous les périphériques correspondant à cette famille. C'est aussi une manière de découpler le socle technique des applicatifs puisque le seul lien existant entre les logiciels embarqués et le terminal est l'API J2ME.

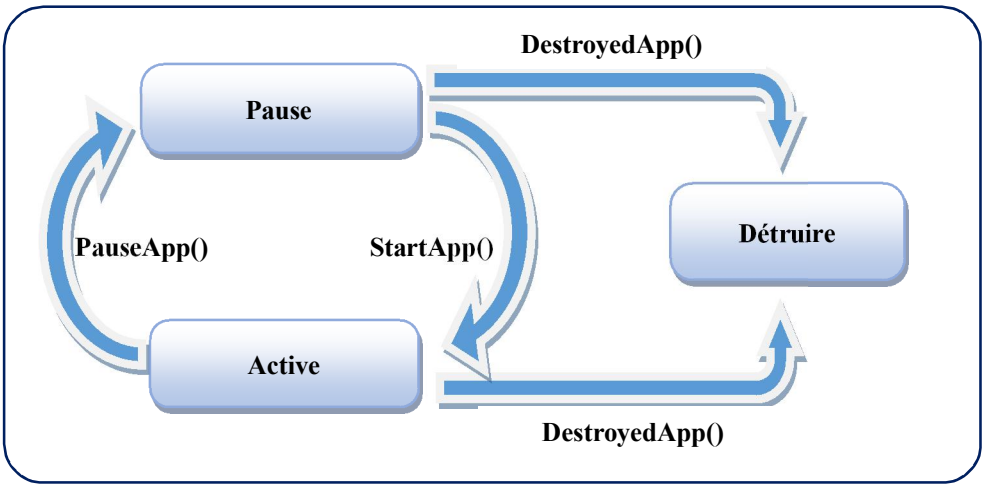


Figure III-3 : Cycle de vie d'une Midlet

StartApp :

C'est la méthode s'appelle par le système pour le mettre une Midlet dans un état Active, ou pour le remettre en service après l'état Paused.

PauseApp :

C'est la méthode qui peut être appelé par le système dans deux cas :

- Si le mobile reçoit un appel.
- Si le mobile manque de mémoire.

Dans le dernier cas, le Midlet doit « libérer » les ressources.

DestroyApp :

C'est une voie « normal » de terminer le travail du Midlet. Cette méthode a un paramètre boolean (unconditional). Ce paramètre montre si l'appel est « inconditionnel ». Autrement dit, si l'appel est égal False et le Midlet n'est pas prêt à terminer son travail, il peut « demander la vie » au système, ayant lancé MidletStateChangeException.

Le système, alors, peut exécuter cette demande, donc, l'état du Midlet ne changera pas. Dans le cas où le paramètre serait égal True, le Midlet doit « obéir » sans « demander la vie », et rendre disponible toutes les ressources.

```
public class Test extends MIDlet {

public Test() {
             //Le constructeur
              }
public void startApp() {
          //ça commence ici au lancement de Test(après le constructeur)
                        }
public void pauseApp() {
          //L'application est en mode "Pause" (pas d'affichage)
                        }

public void destroyApp(boolean unconditional) {
           //Quand on quitte l'application
                                                 }
                                    }
```

Figure III-4 : Architecture d'un programme Midlet

III.3.6. L'interface utilisateur

III.3.6.1. L'interface utilisateur de bas niveau

L'API de bas niveau donne accès direct à l'écran du terminal et aux évènements associés aux touches et système de pointage. Aucun composant d'interface utilisateur n'est disponible : nous devons explicitement dessiner chaque composant, y compris les commandes. Cette API comprend les classes Canvas, Graphics et Font. [26]

- ***La classe Canvas :*** Elle permet d'écrire des applications pouvant accéder aux évènements de saisie de bas niveau tels que :

- Les touches du terminal à qui est associé un code.
- Le pointeur du terminal (s'il en existe un).

Cette classe offre ainsi un grand contrôle sur l'affichage. Les jeux sont la meilleure illustration du type d'application qui utilisera ce mécanisme.

- ***La classe Graphics*** : Elle permet de produire des graphiques en 2D.
- ***La classe Font :*** La classe Font représente les polices de caractères ainsi que les métriques associées.

III.3.6.2. L'interface utilisateur de haut niveau :

L'API de haut niveau fournit quant à elle des composants d'interfaces utilisateurs simples. Mais aucun accès direct à l'écran ou aux évènements de saisie n'est permis. C'est l'implémentation MIDP qui décide de la manière de représenter les composants et du mécanisme de gestion des saisies de l'utilisateur.

Cette API est de loin plus riche en classe que l'API de bas niveau. En effet, elle propose toutes les classes nécessaires au développement d'une interface « classique » sur ce genre de terminal. Les classes « List, ChoiceGroup, TextBox, TextField,DatField et Form permettent un tel développement.

D'autres classes moins « classique » sont également mises à disposition :

- ***La classe Alert :*** Elle met en place une alerte. C'est une boite de dialogue affichant un message textuel, éventuellement accompagné d'une image ou d'un son. Elle permet ainsi d'afficher un avertissement, une erreur, une alarme,… Pendant cet affichage, l'interface utilisateur est désactivée. Si une valeur de time-out a été spécifiée, l'alerte disparait ensuite automatiquement, sinon l'application attend une action de l'utilisateur.
- ***La classe Gauge :*** Elle définit une jauge. Cette dernière permet d'affichée un graphique sous forme de barre dont la longueur correspond à une valeur comprise entre zéro et un maximum.

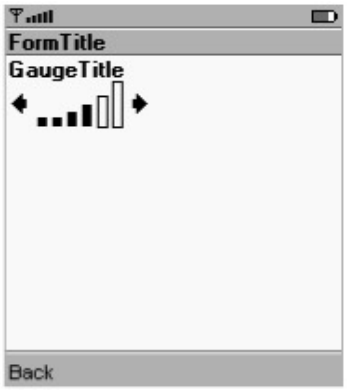


Figure III-5 : la classe Gauge

- ***La classe Ticker :*** Un Ticker est un composant de l'interface utilisateur affichant une ligne de texte défilant à une certaine vitesse.
- ***La classe Command :*** Elle permet de définir une commande, l'équivalent du bouton de commande de windows. Cette classe intègre des informations sémantiques sur une action. Elle possède trois propriétés :

- Le libellé
- Le type de commande (exemple : retour, annulation, validation, sortie, aide, …)
- Le niveau de propriété (qui définit son emplacement et son niveau dans l'arborescence des menus).

Figure III-6 : La Classe command

III.3.7. La connexion réseau

Les principaux atouts d'un terminal sans fil sont sa connectivité et son accessibilité, qui permettent de rester connecté avec le monde entier à tout instant et en tout lieu. Un certain nombre d'améliorations, telles que la couverture du réseau, la bande passante et les technologies sans fil, ont achevé de mettre ces terminaux au gout du jour.

La connectivité est assurée par les outils de connections au réseau de communication. La principale difficulté pour l'API J2ME consiste à intégrer les spécificités de connectivité de chaque famille de terminal. Par exemple, MIDP n'importe que l'implémentation du protocole http, alors qu'un terminal donné peut implémenter d'autres protocoles.

Une autre spécificité très importante pour le réseau est liée aux différents types de réseaux utilisés : réseaux à commutation de paquets ou à commutation de circuits, par exemple.

Les terminaux fonctionnant sur un réseau à commutation de paquets utilisent une communication à base de datagramme, comme UDP (User Data Protocol).

Les informations à envoyer sont dans ce cas découpées en paquets avant d'être transmises puis réassemblées pour être lues. Ce fonctionnement est bien adapter au réseau à capacité fixe mais ne peut pas garantir de qualité de service.

Les terminaux fonctionnant sur un réseau à commutation de circuit utilisent pour leur part une communication à base de socket, comme TCP (Transport Control Protocol). Un circuit est établi dans ce cas entre la source et la destination, et ce circuit reste ouvert pendant toute la durée de la communication. L'intérêt de ce système est qu'il garantit une quantité de service. Son inconvénient est que les ressources utilisées durant l'établissement du circuit sont bloquées et ne peuvent être partagées. [25]

Les interfaces du GCF (Generic Connection Framework) sont organisées sous forme de hiérarchie, comme illustre la figure suivante :

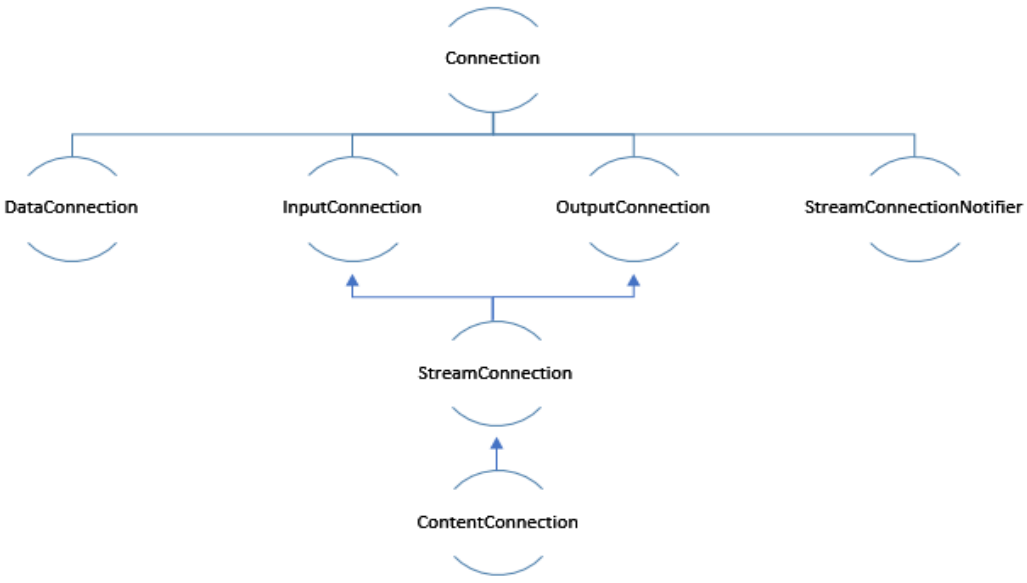


Figure III.7 : Hiérarchie GCF

III.4. Autres outils et langages utilisées

III.4.1. Python

Python est un langage de programmation, dont la première version est sortie en 1991. Créé par Guido van Rossum, il a voyagé du Macintosh de son créateur, qui travaillait à cette époque au Centrum voor Wiskunde en Informatica aux Pays-Bas, jusqu'à se voir associer une

organisation à but non lucratif particulièrement dévouée, la Python Software Foundation, créée en 2001.

Python est un langage puissant, à la fois facile à apprendre et riche en possibilités. Il est, en outre, très facile d'étendre les fonctionnalités existantes. Ainsi, il existe ce qu'on appelle des bibliothèques qui aident le développeur à travailler sur des projets particuliers. Plusieurs bibliothèques peuvent ainsi être installées pour, par exemple, développer des interfaces graphiques en Python.

On peut faire avec Python :

De petits programmes très simples, appelés scripts, chargés d'une mission très précise sur notre ordinateur.

Des programmes complets, comme des jeux, des suites bureautiques, des logiciels multimédias, des clients de messagerie. . .

Des projets très complexes, comme des progiciels (ensemble de plusieurs logiciels pouvant fonctionner ensemble, principalement utilisés dans le monde professionnel). [27]

III.4.1.1. IDLE

IDLE est l'IDE de Python construit avec le Tkinter toolkit graphique, il a les caractéristiques suivantes :

- Codé en 100% pur Python.
- Multi-plateforme: fonctionne sur Windows et Unix
- Multi-fenêtre éditeur de texte avec plusieurs niveaux d'annulation, colorisation Python et de nombreuses autres fonctionnalités
- Fenêtre shell Python.

III.4.2. WAMPSERVER

WAMPSERVER est un ensemble de logiciels permettant de mettre en place facilement un serveur Web. Il s'agit d'une distribution de logiciels libres (Apache MySQL PHP) offrant une bonne souplesse d'utilisation, réputée pour son installation simple et rapide. Ainsi, il est à la portée d'un grand nombre de personnes puisqu'il ne requiert pas de connaissances particulières et fonctionne, de plus, sur les systèmes d'exploitation les plus répandus.

III.4.3. NetBeans

NetBeans est sous licence OpenSource, il permet de développer et déployer rapidement et gratuitement des applications graphiques Swing, des Applets, des JSP/Servlets, des architectures J2EE, dans un environnement fortement personnalisable.

L'IDE NetBeans repose sur un noyau robuste, la plateforme NetBeans, que nous pouvons également utiliser pour développer nos propres applications Java, et un système de plugins performant, qui permet d'avoir un IDE modulable.

A côté de la version complète de l'IDE NetBeans, il existe différentes déclinaisons qui se concentrent sur une plateforme ou un langage précis (Java ME, Java : SE + ME + EE, Ruby, C/C++, PHP).

NetBeans contient, en plus du support pour CVS et SubVersion, un support pour ClearCase, mais aussi pour Mercurial.

Enfin cet IDE possède un débogueur de grande qualité ainsi qu'une interface graphique améliorée.

III.5. Conclusion

Pour conclure, il faut signaler que nous avons utilisé plusieurs outils et langages de programmation pour les besoins de la solution : PHP, HTML pour réaliser le site web, J2ME pour l'application mobile, MySQL pour la gestion de la base de données et enfin PYTHON pour réaliser le serveur SMS.

Cette multitude nous à donner une grande souplesse dans le développement de nos applications vu la puissance et la facilité de manipulation de ses outils.

Chapitre IV Présentation de l'application

IV.1. Introduction

L'objectif de notre travail est de développer une application permettant aux clients d'accéder aux services CCP. Nous proposons trois solutions selon le choix du client : un site web dynamique, une application mobile et un accès par SMS.

Dans ce chapitre on va présenter l'architecture de notre solution et toutes les étapes de la conception de notre application.

IV.2. Architecture globale de solution

Pour accéder aux services CCP le client doit d'abord s'inscrire au site web que nous avons conçu.

Une fois inscrit le client peut accéder à ces services soit à partir du site web ou de l'application mobile comme il peut demander son solde par un SMS.

La figure suivante représente l'architecture globale de solution proposée.

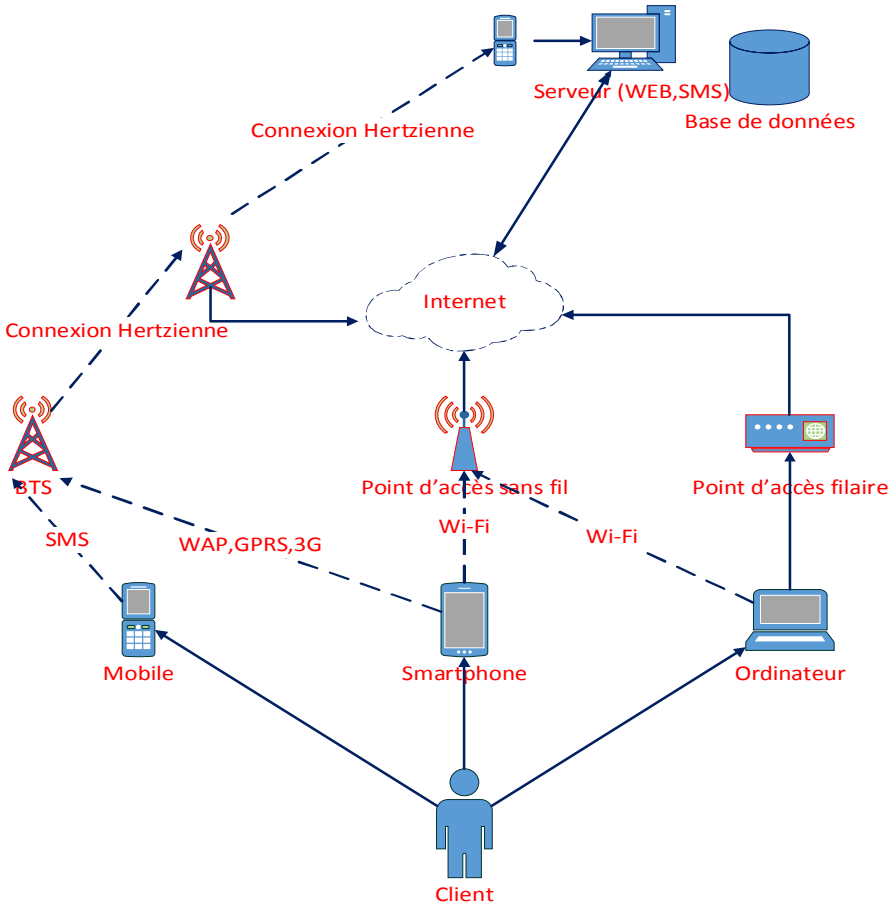


Figure IV-1 : Architecture globale des applications

IV.3. Base de données

Nous avons conçu une base de données MySQL composées de 3 tables (client, compte, historique). La figure IV-2 montre ces trois tables.

La table Compte :

Représente les informations relatives aux opérations effectuées aux comptes clients, le champ solde représente le solde du (client) compte. Elle contient aussi les informations relatives aux commandes clients (demande de carnets de chèques…)

La table Client :

Comporte les informations relatives aux clients, l'index du table est « id » de type INT créé automatiquement par le système, le champ « mdp » est un champ crypté en SHA-1 de type VARCHAR représente le mot de passe de client.

La table historique :

Contient l'historique des opérations effectuées sur un compte, elle sert aussi pour éditer le relevé de compte d'une période définie par le client. La figure suivante montre les différentes tables de base de données.

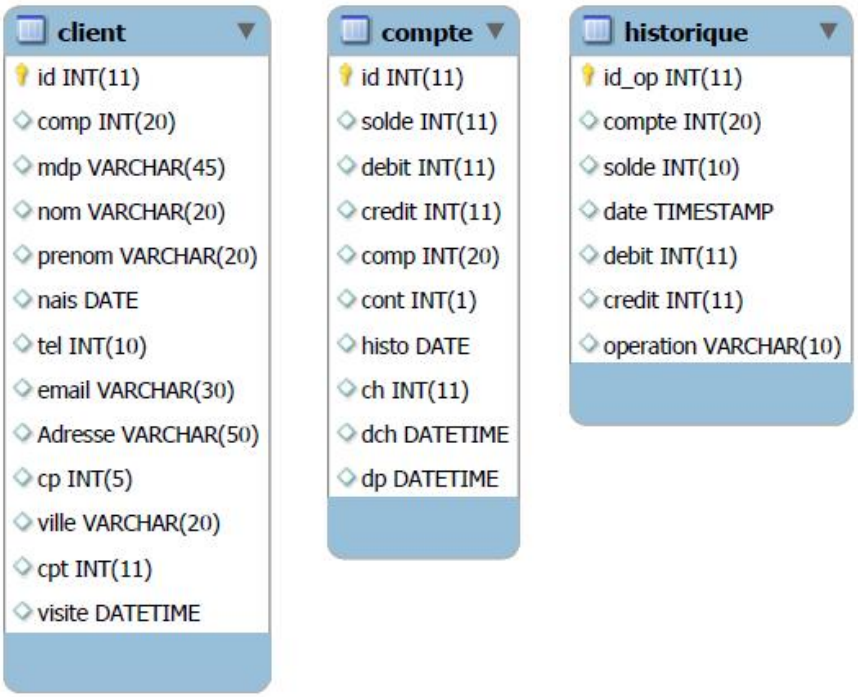


Figure IV-2 : Tables de la base de données.

IV.4. Présentation du site web

IV.4.1. Organigramme du site web

La figure IV-3 montre l'organigramme du site web.

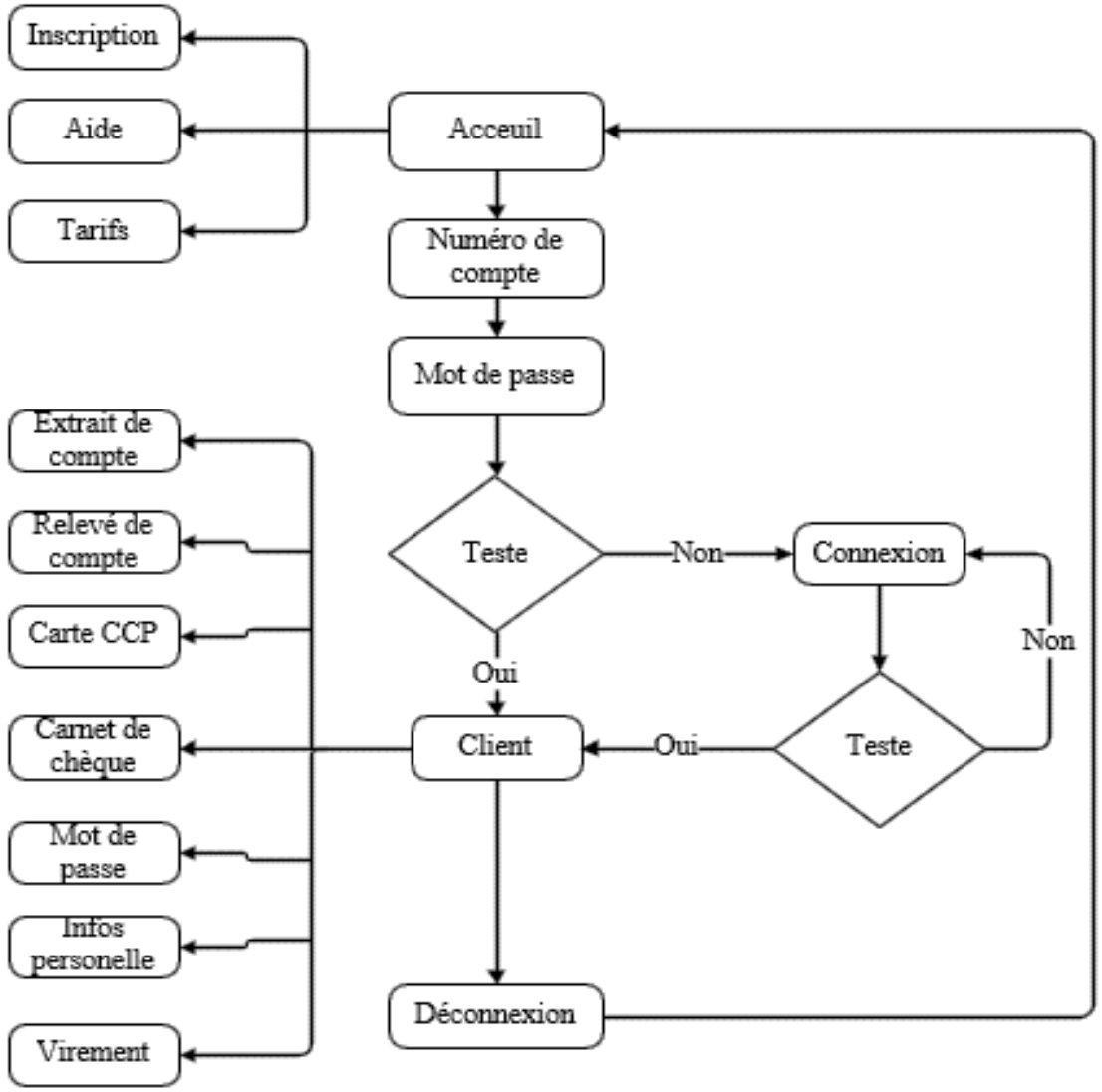


Figure IV-3 : Organigramme du site web

Notre site est divisé en deux parties :

Une partie pour les visiteurs de site contenant :

- Une page d'accueil.
- Une page de connexion.
- Une page pour l'inscription.
- Autres pages (aide, tarifs et page de contact).

Une deuxième partie pour les clients contenant :

- Une page d'accueil.
- Une page de modification de mot de passe.
- La page de mise à jour des informations personnelles.
- La page de commande de carnet de chèques.
- La page de commande de carte à puce.
- La page d'extrait de compte.
- La page de l'historique de compte.
- La page des virements.

IV.4.2. Spécification et réalisation des pages

Dans ce qui suit, nous allons présenter les spécifications précises et les descriptions des pages principales du site.

La page d'accueil :

La figure IV-4 montre la page d'accueil. Elle contient des champs et des liens pour une personne qui veut s'inscrire ou bien pour un abonné qui veut accéder aux services.

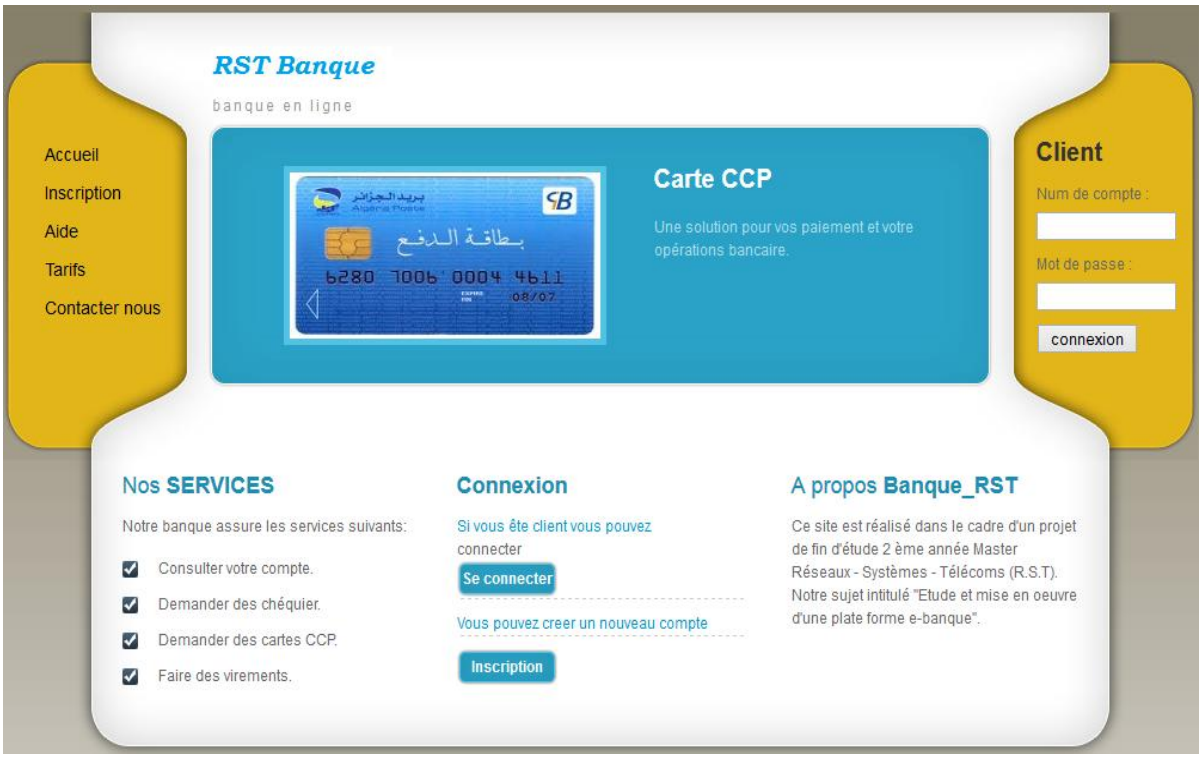


Figure IV-4 : Page d'accueil

La page d'inscription : Cette page est montrée sur la figure IV-5. Après avoir choisi inscription dans la page d'accueil, la page inscription permet au client de s'inscrire en entrant ses informations.

Figure IV-5 : Page d'inscription

Espace de connexion : Pour un client déjà inscrit, il peut accéder à son compte en choisissant se connecter dans la page d'accueil. Une page de connexion s'affiche contenant deux champs que le client devrait remplir, le numéro de compte et le mot de passe.

La figure suivante représente les champs de connexion

Figure IV-6 : Les champs de connexions

Si le numéro du compte et/ou le mot de passe ne sont pas valide un script d'erreur s'affiche.

La page d'index (client) : Après une connexion avec succès le client peut accéder aux différents services proposés, comme par exemple la consultation de compte, relevé de compte demande de carnet de chèque etc.

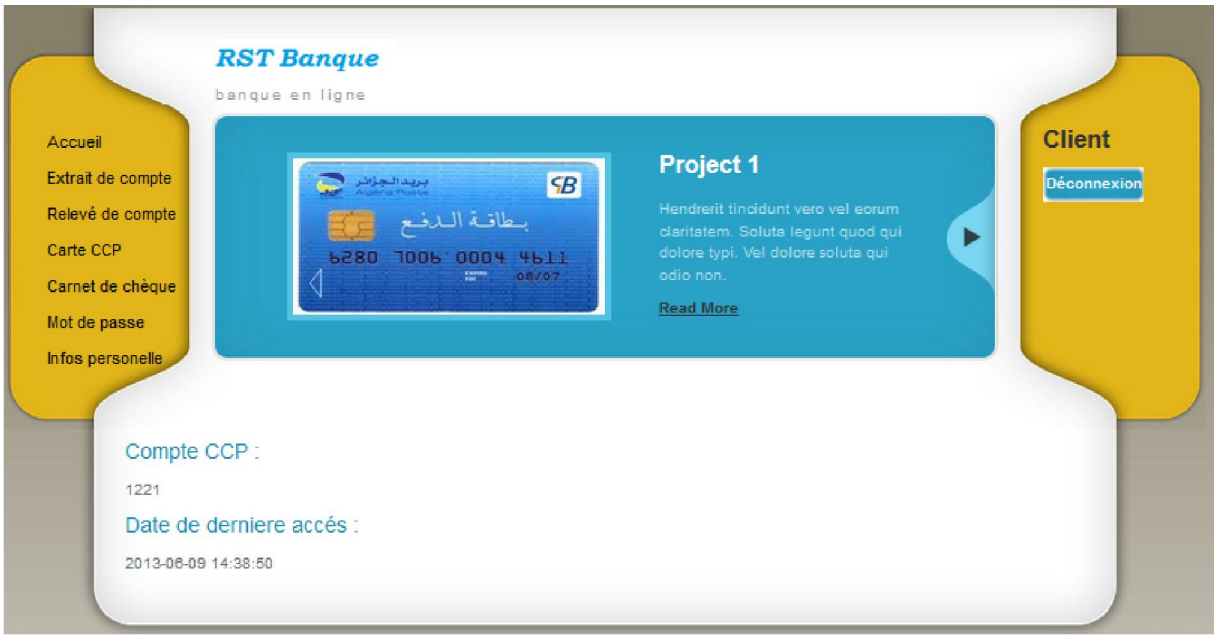


Figure IV-7 : Client/Index.php

Les services que nous offrons sont :

Consultation de crédit :

Num de compte	Solde
1221564360	33600DA

L'historique du compte (le client choisit une période) :

La figure suivante montre la table d'historique

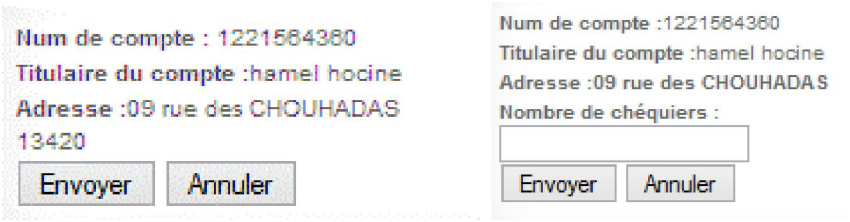

compte n° 1221564360 de 2013-06-09 à 2013-06-15

Num de compte	operation	Solde	debit	credit	Date
1221564360	voir	33620 DA	-10 DA	0 DA	2013-06-09 13:26:02
1221	V.reçue	33820 DA	0 DA	200 DA	2013-06-09 13:27:49
1221	V.effectue	33620 DA	-200 DA	0 DA	2013-06-09 13:31:41
1221564360	voir	33610 DA	-10 DA	0 DA	2013-06-09 18:46:01
1221564360	voir	33600 DA	-10 DA	0 DA	2013-06-10 16:05:49

PDF

Figure IV-8 : La table d'historique.

Demande de carte CCP ou carnet de chèque :



Changement du mot de passe.

Mise à jour des informations personnelles :

Dans cette page le client peut modifier quelques informations comme : l'e-mail et l'adresse,… La figure suivante montre la présentation de la page de modification des informations personnelles.

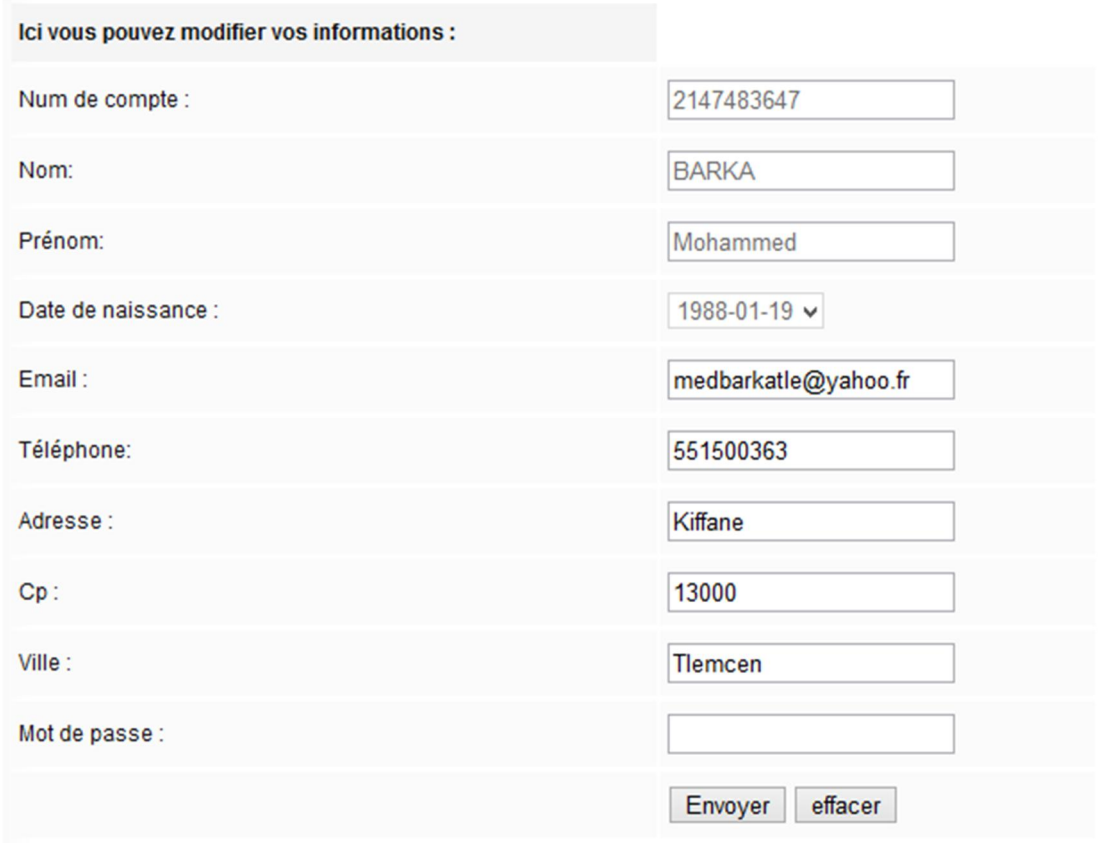
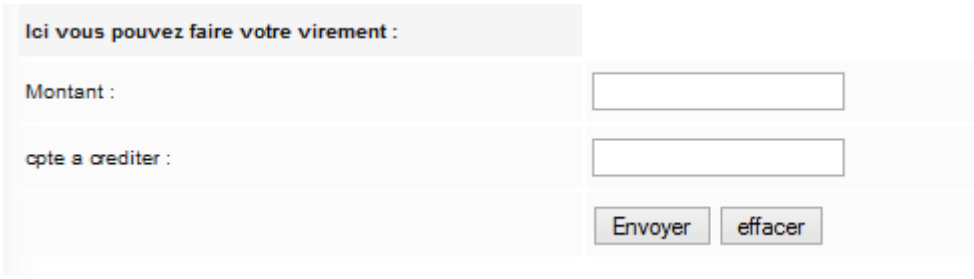


Figure IV-9 : Page de modification des informations personnelles

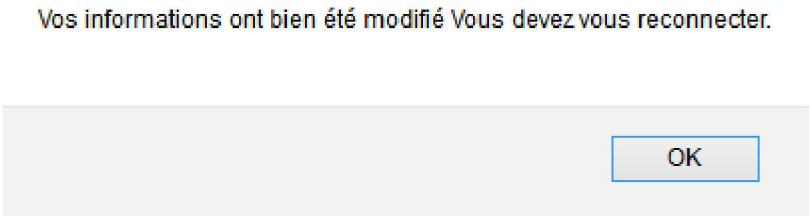
Effectuer des virements :



Les scripts utilisés dans le site :

Pour un nouveau client, un message apparaît en lui demandant de changer son mot de passe, comme le montre la figure suivante.

Dans le cas d'une erreur dans le mot de passe et/ou dans le numéro de compte, d'une utilisation de dix fois le mot de passe ou d'une modification d'informations, un message avertit le client pour chaque cas.



IV.5. Application Mobile (J2ME)

La deuxième partie de notre travail est l'application mobile. Pour accéder aux services CCP, le client se connecte au serveur en utilisant son téléphone mobile. Pour se faire on peut soit concevoir un site WAP en utilisant le XHTML-MP (Mobile Profil) ou concevoir une application mobile (J2ME). Nous avons choisi la deuxième approche qui apporte un gain en temps et en coût.

Pour utiliser cette application il faut que l'utilisateur soit inscrit dans la base de données. Une fois inscrit le client peut télécharger cette application et l'installer sur son téléphone mobile.

IV.5.1. Description des différentes pages de l'application

Parmi plusieurs logiciels existants (Netbeans, Wireless Toolkit, …), nous avons utilisé le logiciel Netbeans 6.5 pour réaliser notre application mobile.

Le diagramme suivant représente la classe application

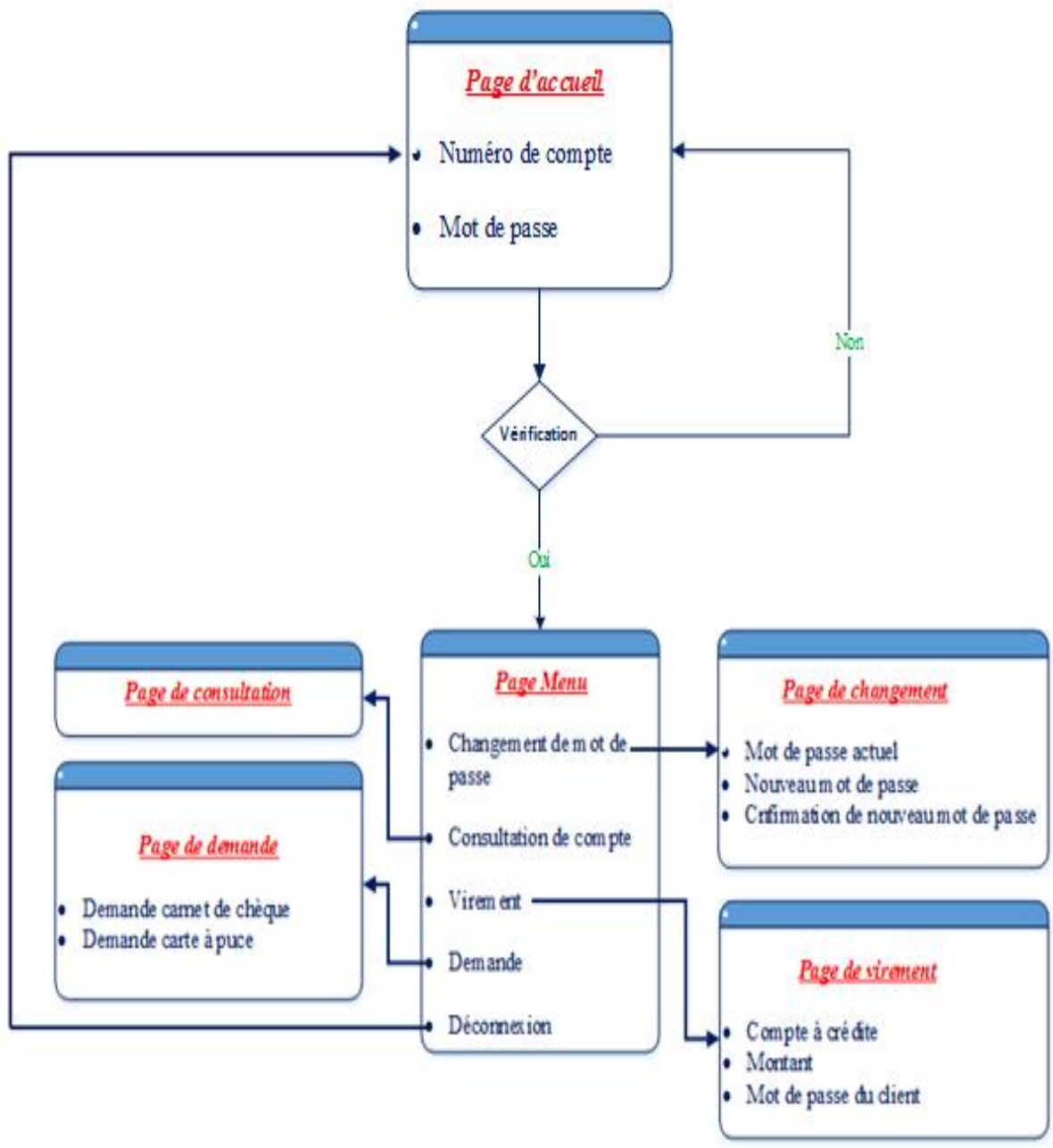


Figure IV-10 : Diagramme de différentes pages de l'application mobile

Une fois que l'application a été installée sur son téléphone mobile, le client peut accéder aux différents services. La figure suivante montre la page d'accueil qui s'affiche sur l'écran du mobile.

Figure IV-11 : Page d'accueil

Plusieurs cas peuvent se présenter :

1er cas : Erreur dans le mot de passe et/ou dans numéro de compte.

La figure suivante montre le message qui s'affiche en cas d'erreur dans le mot de passe et/ou dans numéro de compte.

Figure IV-12: Compte n'existe pas sur la base de données

2eme cas : Echec de connexion

La figure suivante montre les messages qui s'affichent en cas de mot de passe non saisi et/ou le numéro de compte.

Mot de passe non saisi

Numéro de compte non saisi

Les deux champs non saisis

Figure IV-13 : Echec de connexion

3eme cas : Connexion avec succès

La figure suivante s'affiche dans le cas d'une connexion avec succès.

Figure IV-14 : Connexion avec succès

Une fois la connexion établit le client peut effectuer les opérations suivantes :

- Changement de mot de passe.
- Consultation de compte.
- Virement.
- Demande d'un carnet de chèque ou d'une carte à puce.

Le client peut choisir entre plusieurs services proposés, comme le montre la figure suivante.

Figure IV-15 : Services proposés

1-Changement de mot de passe

La figure suivante montre les fenêtres de dialogue qui s'affichent dans le cas où le client demande de changer son mot de passe.

Formulaire pour changer le mot de passe

Confirmation pour le changement de mot de passe

Message montre que le mot de passe a été modifié

Figure IV-16 : Changement de mot de passe.

2-Consultation de compte

En choisissant de consulter le compte, une fenêtre s'affiche donnant le solde du client.

Figure IV-17 : Consultation d'un compte

3-Virement

La figure suivante montre les fenêtres de dialogue qui s'affichent dans le cas où le client demande de faire un virement.

Formulaire pour remplir

Message de confirmation pour le virement

Message montre que le virement est effectué

Figure IV-18 : Virement

4-Demande de carnet de chèque ou carte à puce

Le client peut choisir entre la demande d'un carnet de chèque ou une carte à puce dans la fenêtre qui s'affiche suite à sa demande dans le menu services.

Figure IV-19 : Demande d'un carnet de chèque ou une carte à puce

IV.6. Serveur SMS

La troisième partie de notre travail est l'envoi de SMS. En utilisant le SMS le client peut seulement consulter son solde.

Nous avons choisi de travailler avec le langage Python pour réaliser l'interface de connexion entre le module GSM et le serveur de base de données pour son fiabilité, modularité, facilité d'utilisation et ses fonctionnalités avancées.

Pour permettre à un programme Python de communiquer via le port série, il faut utiliser la bibliothèque pySerial (version-2.6) disponible sur le site officiel de Python.

Notre programme Python communiquera directement avec le module (LG GX200), et communiquera avec le serveur Web via une Base de données MySQL.

Nous avons téléchargé le module MySQL pour Python (MySQL-python-1.2.4b4.win32-py2.7.exe).

IV.6.1. Communication avec le port Série

Notre module est connecté au serveur à travers un port USB. Il communique en réalité par une liaison série, le port USB étant émulé en port série virtuel.

Figure IV-20 : Liaison série mobile –Serveur SMS

Pour envoyer ou récupérer un message SMS il faut d'abord établir la connexion avec le module GSM, le code suivant montre les étapes d'importation du serial.

```
# Importation du module
import serial
# Importation de base de données
import MySQLdb as mdb
# Configuration port serie
ser = serial.Serial(
  port='com5', #selon le numero de COM indiqué dans la
  gestionnaire des périphériques.
baudrate=115200,
parity=serial.PARITY_ODD,
stopbits=serial.STOPBITS_TWO,
bytesize=serial.EIGHTBITS
)
```

IV.6.2. Configuration du module GSM

Une bonne pratique consiste à s'assurer que le module GSM est bien configuré : SMS en format texte et utilisation de l'alphabet Latin. Le code suivant permet d'obtenir cette configuration.

```
ser.write('AT+CMGF=1\r') # SMS format texte
time.sleep(1)
ser.write('AT+CSCS="8859-1"\r') # Alphabet Latin
time.sleep(1)
```

Il est hautement conseillé d'insérer des temps de pause entre l'envoi de plusieurs commandes AT au module GSM.

Le code Python à utiliser pour lire les SMS est le suivant :

```
ser.write('AT+CMGL="REC UNREAD"\r')
out = ""
#  un temps de pause pour attendre la réponse du module
time.sleep(15)
# Lecture des données de la liaison série
while ser.inWaiting() > 0:
   out += ser.read(1)
# enleve la 1ere commande AT
                              longueur = len(out)
                              res = out[23:longueur]
                              index = 1
                              index2 = 0
con = mdb.connect('localhost','root','','rst')
tele = res [index + 0:index + 12]    # NUMERO DE TELEPHONE
print ("tel:"+tele)
cur = con.cursor()
 cur.execute("select solde from compte where tel = "+tele+""):
solde = row[0]
```

Si le message reçu est d'un client inscrit, le système repend par un SMS contenant le solde sinon le programme affiche (numéro de téléphone non trouvé). Le code Python à utiliser pour envoyer un SMS est le suivant :

```
ser.write('AT+CMGS=tel\r')
time.sleep(1)
ser.write('le solde est: ')
ser.write(solde)
ser.write('\r\x1A\r') # équivalent de ctrl+z
time.sleep(1)
```

Exécution de programme :

La figure suivante montre un exemple d'exécution de ce programme

```
Python 2.7.4 (default, Apr  6 2013, 19:54:46) [MSC v.1500 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>> ================================ RESTART ================================
>>>
tel:213774144179
2013/05/12 15:
Appelle-moi STP.
num non trouve
pas de message
pas de message
pas de message
pas de message
tel:213775854219
2013/05/08 11:
Appelle-moi STP.
le solde est:
19980
pas de message
```

Figure IV-21: Exécution du programme

IV.7. Conclusion

La conception et le développement d'application et services sur des périphériques mobiles ne cessent de croitre. Dans ce chapitre nous avons décrit la méthodologie suivie pour la conception de nos applications en présentant les principaux pages constituants les applications, est en montrant la manière dont sont concrétisés les concepts théorique décrits précédemment.

Conclusion générale

Conclusion générale

La conception et le développement d'une solution E-Banking est l'objectif du travail que nous avons effectué. Il s'adresse à toute institution bancaire désireuse d'offrir à ses clients une palette de services basée sur la technologie mobile (SMS, internet,....)

Ce projet nous a donné l'occasion de découvrir le monde bancaire, la technologie du SMS, la téléphonie mobile, les protocoles de communication dans les serveurs de messagerie etc. Ainsi que l'utilisation du SGBD MySQL et plusieurs langages de programmation PHP, HTML, J2ME et PYTHON,…

Cette solution de liaison entre les différents langages de programmation nous parait convenable, parce qu'elle nous a permis de présenter une interface conviviale à tous les utilisateurs et surtout elle permet de disposer d'informations actualisées et nous a facilité la gestion des commandes des clients.

Enfin nous pouvons dire que notre travail est loin d'être complètement achevé, de ce fait plusieurs extensions et perspectives futures restent à atteindre à savoir :

- Effectuer une connexion sécurisée (https) entre l'application mobile et le serveur web.
- Gestion des autres services tels que la demande des carnets de chèques avec un SMS.
- Compléter la partie Mobile pour effectuer une inscription.

Annexe

A) Les commandes AT :

Les commandes AT permettent l'accès aux fonctions d'un téléphone portable par l'intermédiaire d'un terminal.

Ces commandes s'inspirent fortement du standard Hayes, du nom de la société américaine qui dans les années 1970 a défini une liste de commandes universelles permettant de piloter un modem. Chaque instruction débute par les caractères ASCII « AT » tirés de l'abréviation « ATtention » et se termine par un retour chariot, CR :*Carriage Return* , d'où le nom souvent donné à cette série de commandes : instructions « AT ». On peut effectivement comparer un téléphone portable à un modem sans fil, il est donc logique qu'il utilise des instructions semblables au modem fixe qui équipe nos PC. Les constructeurs se doivent de fabriquer des téléphones portables qui respectent ces normes. La première baptisée **GSM07.07** permet l'accès aux fonctions générales du téléphone, la deuxième **GSM07.05** concerne la gestion des SMS.

La figure suivante montre le fonctionnement des commandes AT.

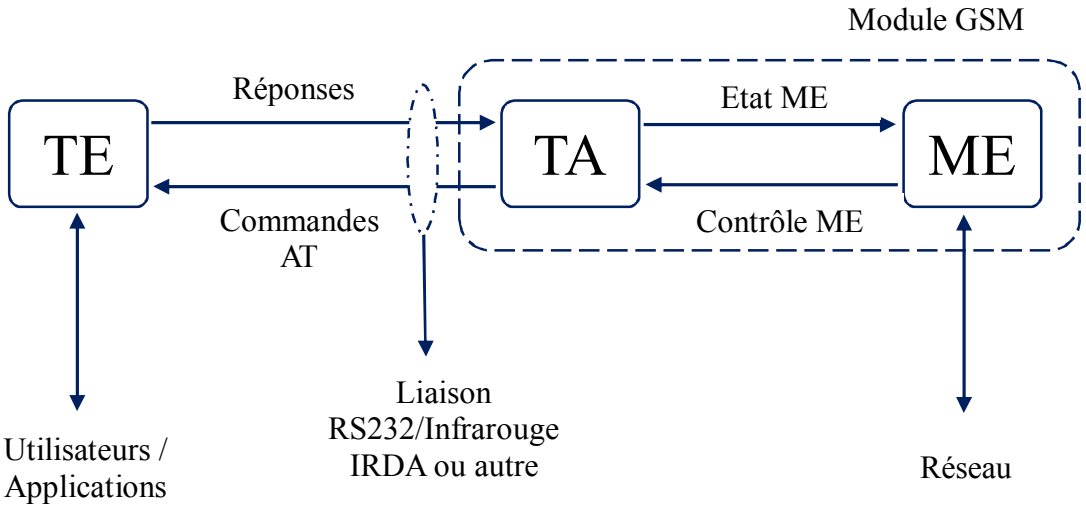


Figure 0A-1 : Les commandes AT

ME (Mobile Equipement) : correspond par exemple à un téléphone portable.

TE (Terminal Equipement) : physiquement peut être un ordinateur ou un microcontrôleur.

TA (Terminal Adaptator) : assure la liaison entre le ME et le TE, à ne pas confondre avec le câble série.

Par exemple on peut utiliser les commandes AT (tableau 1) dans :

- La lecture, l'écriture et la suppression des SMS.
- L'envoi des SMS.
- Contrôler la force du signal.
- Contrôler le statut chargeant et le niveau de charge de la batterie.
- La lecture, l'écriture et la recherche des entrées du répertoire téléphonique.

commande	**Description**
AT	Etablir la connexion avec le modem
AT+CMGS	Envoi d'un message
AT+CMGR	Lecture de message
AT+CMGF	sélection du format du SMS
AT+ CMGL	Liste des messages stockés dans la mémoire
AT+CMGD	Supprimer un message
AT+CMSS	envoi d'un SMS stocké en mémoire
AT+CMGW	écriture d'un SMS

Tableau 0A-1 : Quelque commande AT

Pour tester ces commandes on peut utiliser Hyper Terminal, c'est un petit logiciel de Microsoft utilisé pour envoyer les commandes AT aux modems GSM/GPRS.

Il suffit de le lancer (Démarrer-> Programmes-> Accessoires-> Communications-> Hyper terminal), ensuite choisir les paramètres du port COM auquel est branché le modem et enfin exécuter les commandes AT , dans la figure suivante on voit quelque exemples des commandes AT utilisant Hyper Terminal.

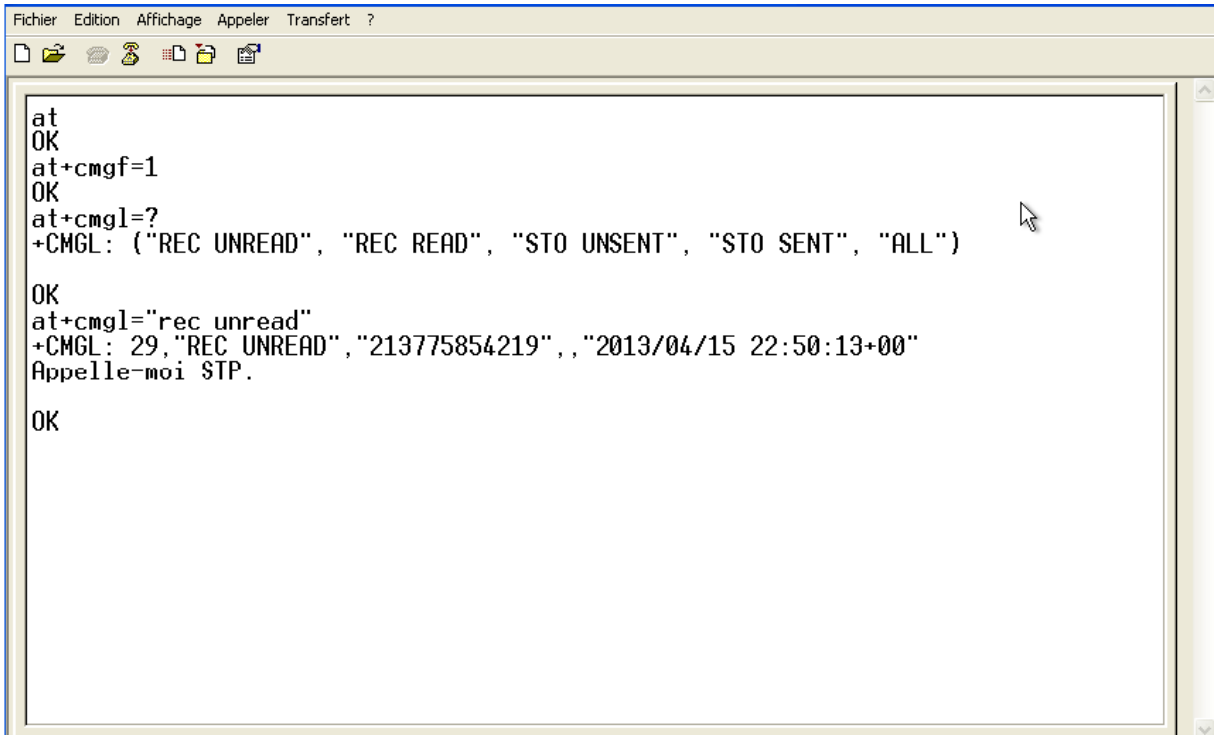


Figure A -2 : Exemple dans Hyperterminal

B) Configuration de HTTPS avec OpenSSL dans WAMP Server :

1- Créer la clé et le certificat SSL

a) ouvrir fenêtre de commande DOS en tapant « CMD » dans votre menu de recherche.

b) tapez : C:\wamp\bin\apache\apache2.2.11\bin

c)créer une clé privée du serveur avec 1 024 bits encryption en saisissant cette commande :

openssl genrsa-des3-out server.key 1024

Il va demander un mot de passe, il suffit d'entrer un mot de passe.

d) supprimer le mot de passe de la clé privée RSA (tout en gardant une copie de sauvegarde du fichier original). Entrez ceci :

copie server.key server.key.org

OpenSSL rsa-en server.key.org-out server.key

Il va demander le mot de passe, il suffit de le taper.

e) créer un certificat auto-signé (X 509 structure) avec la clé RSA, que vous venez de créer. Entrer :

openssl req-new - x 509 - nœuds-sha1-jours 365 - clés server.key-out server.crt - config C:\wamp\bin\apache\apache2.2.11\conf\openssl.cnf

2- Copiez les fichiers server.key et server.crt

a.Dans C:\wamp\bin\apache\apache2.2.11\conf\, créez un dossier nommé ssl.

b. Copiez les fichiers server.key et server.crt dans le dossier ssl.

3- Modifier le fichier httpd.conf, php.ini et httpd_ssl.conf

a. Ouvrir le fichier httpd.conf

b. Retirer le commentaire « # » à la ligne : LoadModule ssl_module modules/mod_ssl.so

c. retirer le commentaire « # » à la ligne : inclure des conf/extra/httpd-ssl.conf

d. Ouvrir le fichier-> C:\wamp\bin\php\php5.3.8\php.ini

e. retirer le commentaire « # » à la ligne : extension=php_openssl.dll

f. Ouvrir le fichier-> C:\wamp\bin\apache\Apache2.2.11\conf\extra\httpd_ssl.conf

g. Rechercher la ligne : < VirtualHost _default_:443 >.

h. juste après :

Remplacer la ligne « DocumentRoot... » par DocumentRoot "C:/wamp/www /"

Modifier la ligne « Nom du serveur... » par ServerName localhost:443

Remplacer la ligne « ErrorLog... » par Errorlog « C:/wamp/bin/apache/Apache2.2.11/logs/sslerror.log»

Remplacer la ligne « TransferLog... » par TransferLog «

C:/wamp/bin/apache/Apache2.2.11/logs/sslaccess.log »

Remplacer la ligne « SSLCertificateFile... » par SSLCertificateFile «

C:/wamp/bin/apache/Apache2.2.11/conf/ssl.crt/server.crt »

Remplacer la ligne « SSLCertificateKeyFile... » par SSLCertificateKeyFile «

C:/wamp/bin/apache/Apache2.2.11/conf/ssl.key/server.key »

Remplacer la ligne < Répertoire « C:/Program Files/Apache Software

Foundation/Apache2.2/cgi-bin » > par < Répertoire « C:/wamp/www / ">

Ajouter les lignes suivantes à l'intérieur de ces balises <Directory... >...</Directory> :

Options Indexes FollowSymLinks MultiViews

AllowOverride All

Ordre permettre, refuser

Allow from all

Remplacer la ligne « CustomLog... » par CustomLog «

C:/wamp/bin/apache/Apache2.2.11/logs/ssl_request.log »

4- S'assurer que cela fonctionne !

a. dans la fenêtre de commande DOS précédente, taper httpd -t. S'il affiche Sysntax est OK, puis passé à l'étape suivante. Si ce n'est pas le cas, corriger la syntaxe erronée et refaire l'étape 3.

b. Redémarrer le serveur Apache. Si le redémarrage est réussie, ouvrir le navigateur et entrer https://localhost/

Capture d'écran :

La figure suivante représente l'écran d'accueil après la configuration de https

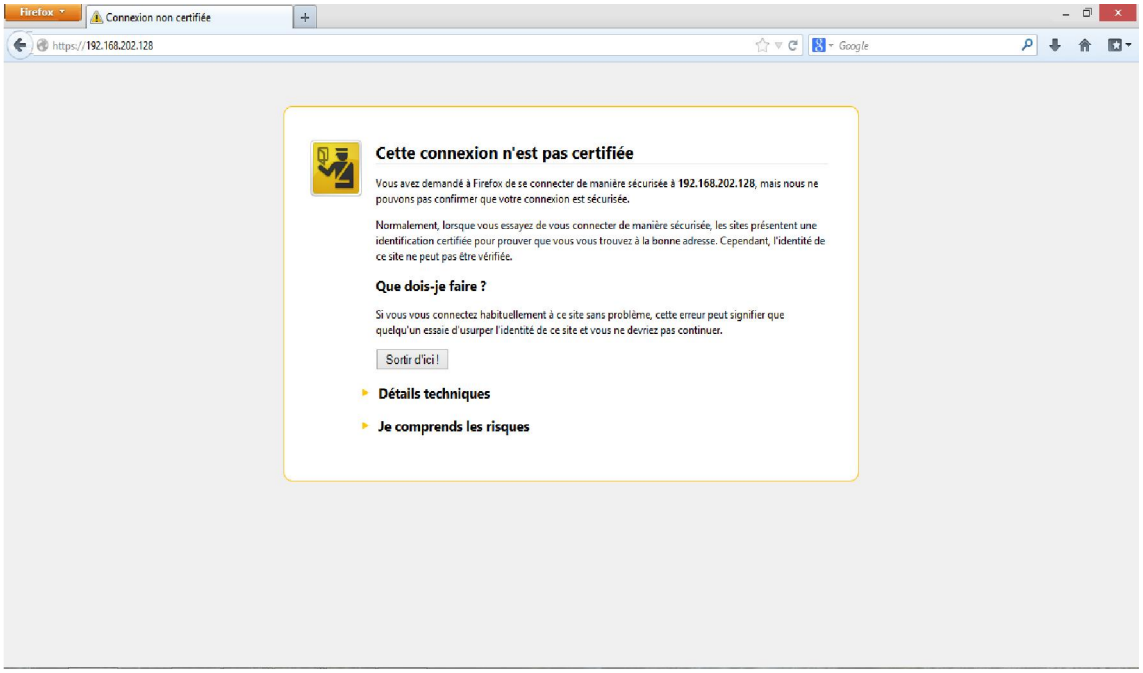


Figure B-1 : Ecran d'accueil après la configuration de https

La page d'accueil de Wamp server après accepter le certificat comme le montre la figure suivante :

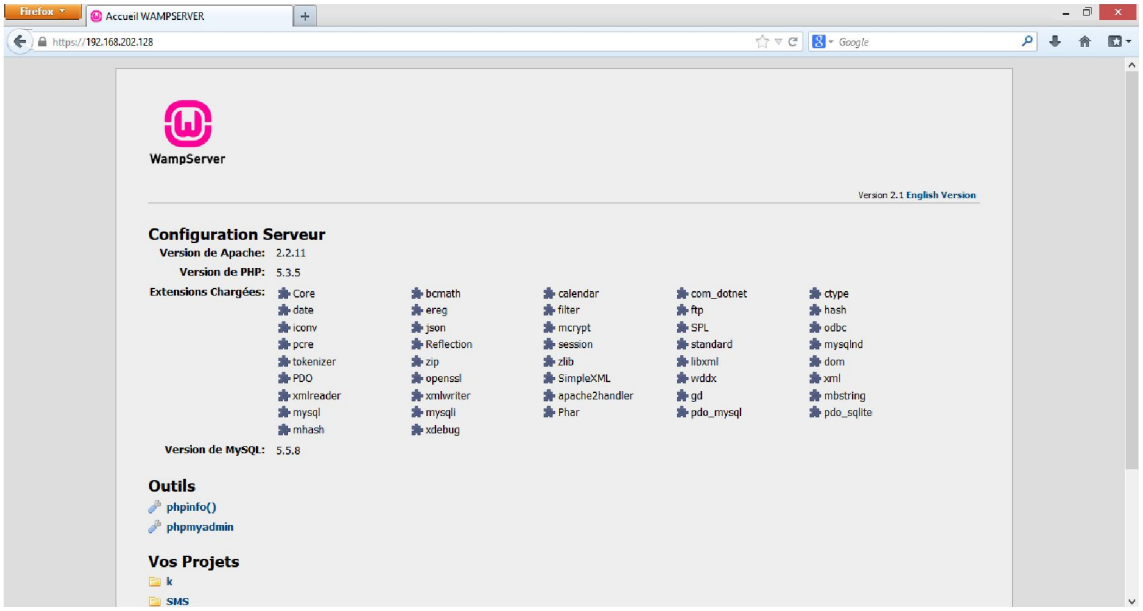


Figure B-2 : Page d'accueil de Wamp server après accepter le certificat

C) Html5 <http://41mag.fr />

BALISE	ATTRIBUT / DESCRIPTION		
`<!-- Commentaire -->`	*Commentaire*		
`<!DOCTYPE html>`	*Déclaration du Doctype*		
BALISE DE PREMIER NIVEAU – *Code minimal d'une page web*			
`<html>`	*Indquez au naigateur que le document est en HTML*		
`<head>`	*En-tête de la page*	`<body>`	*Corps de la page*
BALISE D'EN-TÊTE – *Entre les balises <head>*			
`<title>`	Titre de la page, tres important pour le référencement		
`<script>`	Inserer script	`<style>`	Inserer CSS
`<noscript>`	Message à afficher si le script n'est pas toleré		
`<base />`	URL par défaut `<base href="http://41mag.fr/" target="_blank" />`		
`<link />`	CSS	`<link rel="stylesheet" type="text/css" href="#" />`	
	PAGE	`<link rel="start" href="index.html" />`	
	RSS	`<link rel="alternate" type="application/rss+xml" href="#" />`	
	FAVICON	`<link rel="shortcut icon" type="image/x-icon" href="#" />`	
`<meta />`	TITLE	Titre de la page	
	DESCRIPTION	Description de la page	
	KEYWORDS	Mots-clés de la page	
	ROBOTS	Restrictions pour les robots	
	SYNDICATION-SOURCE	Indique l'URL d'origine	
	ORIGINAL-SOURCE	Indique que c'est l'orignial	
	NOTRANSLATE	Ne sera pas traduit	
	HTTP-EQUIV CHARSET	Jeux de caractères	
	HTTP-EQUIV REFRESH	Raffraichir la page	
	HTTP-EQUIV PRAGMA	Définit le cache du navig.	
BALISE D'ARCHITECTURE			
`<header>`	Définit l'en-tête d'une section ou d'une page		
`<footer>`	Définit le bas d'une section ou d'une page		
`<hgroup>`	Définit les informations d'en-tete d'une section ou d'une page		
`<details>`	Définit les détails d'un élément		
`<summary>`	Définit l'en-tête des details d'un élément		
`<menu>`	Définit un menu en forme de liste		
`<section>`	Définit une section		
`<article>`	Définit un article		
`<aside>`	Définit un élément latéral		
`<nav>`	Définit un groupe de liens de navigations		
`<iframe>`	Introduis une page html dans une frame		
`<div>`	Calque ou section		
`<span>`	Section de type inline		
BALISE DE STRUCTURATION DE DE TEXTE			
`<h1> à <h6>`	Créer un titre		
`<p>`	Paragraphe	`<a>`	Lien
`<strong>`	Mise en exergue	`<b>`	Texte en gras
`<em>`	Italique en exergue	`<i>`	italique
`<mark>`	Marqueur de texte	`<small>`	Rétrécis le texte
`<sub>`	Mise en indice	`<sup>`	Mise en Exposant
`<adress>`	Définit une adresse	`<cite>`	Citation
`<abbr>`	Abréviation	`<dfn>`	Définition
`<del>`	Texte supprimé	`<ins>`	Texte ajouté
`<time>`	Date / Horaire	`<meter>`	Mesure
`<code>`	Portion de code	`<pre>`	Texte préformaté
` `	Saut de ligne	`<wbr>`	Empl pr saut 2 ligne
`<blockquote>`	Longue citation	`<q>`	Courte citation
`<samp>`	Echantillon	`<var>`	Variable
`<kbd>`	Raccourci clavier	`<bdo>`	Sens du texte

BALISE	ATTRIBUT / DESCRIPTION		
BALISE DE LISTE			
`<ul>`	Liste non-ordonné	`<ol>`	Liste ordonné
`<li>`	Elément de liste	`<dl>`	Liste de définition
`<dt>`	Terme à definir	`<dd>`	Définition du terme
BALISE DE TABLEAU			
`<table>`	Tableau	`<caption>`	Titre du tableau
`<thead>`	En-tête du tableau	`<tbody>`	Corps du tableau
`<tr>`	Ligne du tableau	`<th>`	Cellule d'en-tête
`<td>`	Cellule du tableau	`<tfoot>`	Bas du tableau
`<col>`	Colonne du tableau	`<colgroup>`	Groupe de colonne
BALISE DE FORMULAIRE			
`<form>`	Formulaire	`<fieldset>`	Regroupe plusieurs elémnts du formulaire
`<legend>`	Titre d'un groupe	`<label>`	Titre d'un élément
`<datalist>`	Liste déroulante	`<select>`	Liste selectionnable
`<option>`	Elémént d'une liste	`<optgroup>`	Grp d'élmnts d'une list
`<textarea>`	Zone de texte	`<keygen>`	Génération d'une clé
`<button>`	Bouton cliquable	`<command>`	Bouton de commande
`<output>`	Définit un type de sortie		
`<input />`	button	file	radio	text
	checkbox	hidden	range	time
	color	image	reset	url
	date	month	search	
	datetime	number	submit	
	email	password	tel	
BALISE MULTIMEDIA			
`<area>`	Zone cliquable à l'interieur d'une image		
`<audio>`	Contenu audio	`<canvas>`	Graphique
`<img />`	Image ou photo	`<progress>`	Progression
`<figure>`	Groupe d'element multimédia	`<ficaption>`	Légende du groupe d'élément
`<video>`	Vidéo	`<source>`	Source du media
`<map>`	Carte / image	`<param>`	Parametre d'objet
`<embed />`	Contenu exterieur	`<object>`	Objet du cont. ext
AUTRE			
`<rp>`	Annotation pr le nav	`<rt>`	Explication ruby
`<ruby>`	Annotation ruby	`<hr />`	Barre horizontale

ATTRIBUT STANDAR			
Acceskey	Raccourci clavier	**itemprop**	Utilisé pr un gp d'élémnt
class	Attribut une classe	**context-menu**	Menu contextuel d'elemnt
lang	Langage d'un élément	**spellcheck**	Correction automatique
data-	Définit un attribut	**style**	Applique un style
dir	Direction du texte	**subject**	Définit l'elmnt correspondt
draggable	Element deplacable	**tabindex**	Définit l'ordre d'un tabl0
hidden	Element caché	**title**	Titre de l'élément
id	Nomme un élément	**conteneditable**	Element editable
item	Utilisé pour un groupe d'élément		

EVENEMENT			
Pour la balise <body>	**Pour formulaire**	**Pour la souris**	**Pour les medias**
Onafterprint, onbeforeprint, onafterload, onblur, onerror, onfocus, onhaschange, onload, onmessage, onoffline, ononline, onpagehide, onpageshow, onpopstate, onredo, onresize, onstorage, onundo, onunload	Onblur, onchange, oncontextmenu, onfocus, onformchange, onforminput, oninput, oninvalide, onsubmit, onselect	Onclick, ondblclick, ondrag, ondragend, ondragenter, ondragleave, ondragover, ondragstart, ondrop, onmousedown, onmouseup, onmousemove, onmouseout, onmousewhell, onscroll	Onabort, oncanplay, oncanplaytrought, ondurationchange, onemptied, onended, onerror, onloaddata, onloadstart, onpause, onplay, onplaying, onprogress, onseeked, onsuspend, onwaiting, onvolumechange

d) Détails des principales commandes MySQL

www.41MAG.fr

Fonction	Définition	Explication
CONNEXION A LA BASE DE DONNEES		
mysql_connect	Connexion a MySQL Connexion a la base de donnes	mysql_connect("nom_de_l'hote", "login", "mot_de_passe"); *Nom de l'hote : IP de l'ordinateur ou MySQL est installé. mettre "localhost"* *Login : Il permet de vous identifier. Se renseignez auprès de votre hébergeur.* *Mot de passe : Généralement c'est le même que celui pour accéder au FTP* Ex: mysql_connect("localhost", "41mag", "enzo81"); ==> Script pour **WAMP** : mysql_connect("localhost", "root", "");
mysql_select_db	Selection de la base de données	mysql_select_db("nom_de_base"); *// Sélection de la base nom_de_base*
sql_close	Déconnexion de la base de données	**<?php** mysql_connect("localhost", "nom_de_base", "mot_de_passe"); *// Connexion à MySQL* mysql_select_db("nom_de_base"); *// Sélection de la base 41mag* *// On est connectés, on peut travailler sur la BDD* mysql_close(); *// On a fini de travailler, on ferme la connexion Déconnexion de MySQL* **?>**
RECUPERATION DE DONNEES		
mysql_query	Définition d'une requete	*//La fonction renvoie une valeur, la variable $reponse récupère ce que MySQL renvoie.* $reponse = mysql_query("Requete SQL"); Exemple : $reponse = mysql_query("SELECT * FROM nom_de_la_base"); **=> SELECT :** *En SQL, le premier mot indique quel type d'opération doit faire MySQL. Ici, SELECT demande à MySQL d'afficher ce que contient une table.* *=> * : Après le SELECT, on doit indiquer quels champs MySQL doit récupérer dans la table. Si on n'est intéressé par les champs "nom" et "adresse", il faudra taper :* **SELECT** nom, adresse **FROM** nom_de_la_base *Si vous voulez prendre tous les champs, tapez *. Cette étoile se traduit par "tout"* **=> FROM :** *Se traduit par "dans". FROM fait la liaison entre le nom des champs et le nom de la table* **=> nom_de_la_base :** *Nom de la table dans laquelle il faut aller piocher les donnees.*

mysql_fetch_array	Afficher le resultat d'une requete	*$reponse contient quelque chose d'inexploitable. mysql_fetch_array va créer un array à partir de $reponse. Un tableau associatif : mettre entre crochets le nom du champ qui vous intéresse. Par exemple, pour le champ "adresse", utiliser l'array $donnees['adresse'].*
		<?php
		mysql_connect("localhost", "41mag", "mot_de_passe"); *// Connexion à MySQL*
		mysql_select_db("nom_de_la_base"); *// Sélection de la base coursphp*
		$reponse = mysql_query("SELECT * FROM jeux_videos"); *// Requête SQL*
		// Avec cette boucle, on liste tous ce que contient la table
		while ($donnees = mysql_fetch_array($reponse))
		{ *// La boucle affiche permet d'afficher toute les entres a la suite*
		?>
		Mr **<?php** echo $donnees['nom']; **?>** habite à l'adresse suivante : **<?php** echo $donnees['adresse']; **?>**
		
		<?php
		}
		mysql_close(); *// Déconnexion de MySQL*
		?>

or die(mysql_error())	Afficher le détail des erreurs	*Lorsqu'une requête SQL "plante",PHP indique l'erreur à la ligne du mysql_fetch_array. Ce n'est pas tres precis. Pour afficher des détails sur une erreur, prenez l'habitude de rajouter le code or die(mysql_error()) sur la même ligne que vos mysql_query.* $reponse = mysql_query("SELECT * FROM jeux_videos") or die(mysql_error()); *Ce code rajouté ne fera rien s'il n'y a pas d'erreur.*

Fonction	Définition	Explication
CRITERES DE SELECTIONS		

WHERE	Triage des données	**SELECT * FROM** jeux_videos **WHERE** possesseur='Enzo'
		Traduction : Sélectionner tous les champs de la table jeux_videos lorsque le champ possesseur est égal à Enzo.
		
		$reponse = mysql_query("SELECT nom, propietaire FROM jeux_videos WHERE propietaire='Enzo'"); *// Sélectionnons les champs nom et possesseur de la table "jeux_videos", uniquement lorsque le jeu appartient à Enzo*
		
		while ($donnees = mysql_fetch_array($reponse)) *// Attention au parenthese*
		{ **?>**
		
		<?php echo $donnees['nom']; **?>** appartient à **<?php** echo $donnees['propietaire']; **?>**
		
		<?php
		}
		?>

ORDER BY	Ordonne les résultats	**SELECT * FROM** jeux_videos **ORDER BY** prix
		Traduction : Sélectionner tous les champs de la table jeux_videos, et ordonner les résultats par prix croissant.
		
		SELECT * FROM jeux_videos **ORDER BY** prix **DESC**
		*Pour classer les resutat par ordre **DECROISSANT**, il faut rajouter DESC a a fin.*
		
		*Si on utilise ORDER BY sur un champ qui contient du texte, le classement est fait par ordre **alphabétique**.*
		
		$reponse = mysql_query("SELECT nom, prix FROM jeux_videos ORDER BY prix"); *// Sélectionner les champs 'nom' et 'prix' de jeux_videos et classer les résultats par prix.*
		
		while ($donnees = mysql_fetch_array($reponse))
		{ **?>**
		
		<?php echo $donnees['nom']; **?>** coûte **<?php** echo $donnees['prix']; **?>** €
		
		<?php
		}
		?>

LIMIT	Selection d'une partie des resultats	**SELECT * FROM** jeux_videos **LIMIT** 0, 20
		Traduction : Le premier chiffre, ici le "0", indique a partir de quelle entree on commence a lire la table. LE deuxieme chiffre, ici le "20", indique le nombre d'entree a selectionner.
		
		// Sélectionner les 10 premières entrées de la table jeux_videos
		$reponse = mysql_query("SELECT nom FROM jeux_videos LIMIT 0, 10");
		
		echo "Voici les 10 premièr jeux de la table jeux_videos :<p>";
		
		while ($donnees = mysql_fetch_array($reponse))
		{ **?>**
		
		<?php echo $donnees['nom']; **?>**
		
		<?php
		}
		?>

	Condition multiple	**SELECT * FROM** jeux_videos **WHERE** possesseur='Enzo' **AND** prix < 50 *Traduction : Sélectionner tous les champs de jeux_videos lorsque le possesseur est Enzo ET lorsque le prix est inférieur à 50"* **SELECT** nom, console, prix **FROM** jeux_videos **WHERE** console='PSP' OR console='PS3' **ORDER BY** prix **DESC LIMIT** 0,10 Remarque : Il faut utiliser les mots-clés dans l'ordre suivant : **WHERE** puis **ORDER BY** puis **LIMIT**, sinon MySQL ne comprendra pas votre requête.

<table>
<tr><th>Fonctions</th><th>Définition</th><th>Explication</th></tr>
<tr><td>COUNT</td><td>Calcul du nombre d'entree dans la base de données</td><td>
<?php
mysql_connect("localhost", "41mag", "mot_de_passe");
mysql_select_db("maBase");

// Combien d'entrées dans jeux_vidéos ?
$retour = mysql_query("SELECT COUNT(*) AS nbre_entrees FROM jeux_videos");
$donnees = mysql_fetch_array($retour);
?>

Il y a <?php echo $donnees['nbre_entrees']; ?> jeux vidéos dans la BDD !

<?php
mysql_close(); // Déconnexion de MySQL
?>
</td></tr>
<tr><td colspan="3">MODIFIER LES DONNEES</td></tr>
<tr><td>INSERT INTO</td><td>Ajouter des données</td><td>
INSERT INTO nom_de_la_table(champ1, champ2, champ3 etc...)
VALUES('valeur relative au champ1', 'valeur relative au champ2', etc...)
// Pour le champ ID ne rien mettre entre les apostrophe, si vous avez cocher l'option auto-increment. Mysql genere les nombres dans l'ordres.

Ecriture réduite :

INSERT INTO nom_de_la_table VALUES('valeur relative au champ1', 'valeur relative au champ2', etc...) // Attention a bien respecter l'ordre de champs.

<?php
mysql_connect("localhost", "41mag", "mot_de_passe");
mysql_select_db("maBase");

mysql_query("INSERT INTO jeux_videos VALUES('', 'fifa12', 'Enzo', 'PS3', '45', '50', 'jeux de foot')"); // ajoute une entrée dans la BDD pour le jeu "Bfifa12", appartenant à "Enzo", qui fonctionne sur "PS3", qui coûte "45" euros etc...

mysql_close();
?>
</td></tr>
<tr><td>UPDATE</td><td>Modifier des données</td><td>
UPDATE nom_de_la_table SET champ="nouvelle valeur", champ"nouvelle valeur" WHERE champ="valeur repere"

Exemple :
UPDATE jeux_videos SET prix='10', nbre_joueurs_max='32' WHERE ID='51'

Exemple:
UPDATE jeux_videos SET possesseur='Enzo' WHERE possesseur='Michel'
Traduction : Dans la table jeux_videos, modifier toutes les entrées dont le champ possesseur est égal à Michel, et le remplacer par Enzo. Qu'il y ait 1, 10, 100 ou 1000 entrées, cette requête à elle-seule suffit pour mettre à jour toute la table.
</td></tr>
<tr><td>DELETE</td><td>Supprimer des données</td><td>
DELETE FROM nom_de_la_table WHERE nom_de_l'entree="valeur de l'entre"

Attention : WHERE est indispensable pour indiquer quelle(s) entrée(s) doivent être supprimée(s). Si vous l'oubliez, tout sera supprimé ! Cela équivaut à vider la table.

A utiliser avec ATTENTION

Exemple :
DELETE FROM jeux_videos WHERE nom='fifa12'
</td></tr>
</table>

Bibliographie

Bibliographie

[1] I. Boutekdjiret et Z. Mezrague , CONCEPTION ET REALISATION D'UNE SOLUTION SMS BANKING POUR TRUST BANK ALGERIA, 2008.

[2] «What is online banking ?,» 2013. [En ligne]. Available: http://www.investorwords.com/3420/online_banking.html.

[3] «Guichet automatique bancaire,» 7 6 2013. [En ligne]. Available: http://fr.wikipedia.org/wiki/Guichet_automatique_bancaire.

[4] A. AYADI, «Inovations technologique dans les réseaux mobiles,» 2004.

[5] M. T. VALERIE, SECURITE APPLIQUEE AUX MESSAGES DANS LES SERVICES, 2008.

[6] «Le stnadard GSM,» 12 05 2013. [En ligne]. Available: http://www.commentcamarche.net/contents/1122-le-standard-gsm.

[7] G. Pujolle, LES RÉSEAUX, editions-eyrolles, 2008.

[8] A. H. Hassan, Etude et Conception d'une solution de SMS Banking, 2011.

[9] SA, «Qu'est ce qu'une carte CIB ?,» 22 05 13. [En ligne]. Available: http://www.satim-dz.com/carte-cib.html.

[10] «Algérie poste,» [En ligne]. Available: eccp.poste.dz.

[11] «Qu'est ce que le service Racidi ?,» [En ligne]. Available: http://www.mobilis.dz/particulier/service.php?page=11. [Accès le 14 mai 2013].

[12] A. F. COULIBALY et N. MALLE , Accès à lèinternet pour les mobiles, ORAN, 2005.

[13] P. ATELIN, Réseaux informatiques , notions fondamentales, éditions eni, 2008.

[14] . L. Stéphane et . P. Dominique, INTERNET :SERVICES ET RÉSEAUX, Dunod, 2004.

[15] «Transport Layer Security,» 26 mai 2013. [En ligne]. Available: http://fr.wikipedia.org/wiki/Transport_Layer_Security.

[16] S. Bruce , Cryptographie_appliquee, Vuibert Informatique.

[17] P. Thomas et A. Hélaïli, Construire une application WAP, EYROLLES, 2001.

[18] D. boutton, Créer un site e-commerce avec Dreamweaver CS4 et PHP/MySQL, Person education France, 2009.

[19] B. Mohammed, Conception et réalisation d'un site web pour l'enseignement à distance e-Learning, alger, 2007.

[20] J. CARFANTAN, PHP & MySQL et CSS, MICRO APPLICATION, 2009.

[21] J. Pardanaud, Dynamisez vos sites web avec Javascript, Site du zero, 2012.

[22] F. DRAILLARD, Premiers pas en CSS et XHTML 2eme édition, EYROLLES, 2008.

[23] R. Grin, «Langage SQL,» 2008.

[24] B. Delb, J2ME : Applications Java pour terminaux mobiles, EYROLLES, 2001.

[25] D. Mohammed, La préinscription des étudiants via un téléphone mobile, Tlemcen , 2009.

[26] J.-M. DOUDOUX, «Développons en Java 1.90,» 13 02 2013. [En ligne]. Available: http://jmdoudoux.developpez.com/cours/developpons/java/.

[27] T. Ziadé, Programmation PYTHON, EYROLLES, 2009.

Acronymes

Acronymes

API	Application Programming Interface
ARPANET	Advanced Research Projects Agency Network
ASC	Auto-Search Channel
ASCII	American Standard Code for Information Inter change
AUC	Authentification Center
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CDC	Connected Device Configuration
CERN	Centre Européen de Recherche Nucléaire
CIB	Carte Bancaire
CLDC	Connected Limited Device Configuration
CSS	Cascading Style Sheets
CVS	Concurrent Versions System
EIR	Equipement Identity Register
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfert Protocol
HTTPD	Hypertext Transfer Protocol Daemon
HTTPS	Hyper Text Transfer Protocol Secure
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity

IP	Internet Protocol
ISP	Internet Service Provider
JAD	Java Decompiler
JAR	Java ARchive
JME	Java Micro Edition
KVM	Kilobyte Virtual Machine
KVM	KiloByte Virtual Machine
MD5	Message Digest 5
ME	Mobile Equipement
MILNET	Military Network
MS	Mobile Station
MSC	Mobile Switching Center
NAS	Network Attached Storage
NSFNet	National Science Foundation Network
NSS	Network Station Subsystem
OMC	Organisation mondiale du commerce
OSI	Open Systems Interconnection
PHP	Hypertext Preprocessor,Personal Home Pages
RFC	Request For Comment
RTC	Réseau Téléphonique Commuté
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMS	Short Message Service
SMSC	Short Message Service Center
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SRES	Signature Response
SSL	Secure Sockets Layer
TA	Terminal Adaptator
TCP	Transmission Control Protocol
TE	Terminal Equipement
TLS	Transport Layer Security

UDP	Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VLR	Visitor Location Register
WAE	Wireless Application Environnent
WAP	Wireless Application Protocol
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WLTS	Wireless Transport Layer Secure
WML	Wireless Markup Language
WSP	Wireless Session Protocol
WTA	Wireless Telephony Application
WTP	Wireless Transaction Protocol
WWW	World Wide Web

Résumé :

L'explosion du nombre de terminaux mobiles dans le monde, au point de dépasser celui des ordinateurs, est un fait économique important. Avec les nouveaux réseaux de télécommunication et l'accroissement des capacités de traitement des terminaux, de nouvelles possibilités d'interagir et de communiquer avec les clients, y compris via le réseau Internet, ont fait leur apparition. Ainsi, l'Internet Mobile apporte des opportunités d'élargissement de la palette des services proposés par les banques.

L'amélioration de ces techniques électroniques du système bancaire a pour but de faire face aux défis de l'ère moderne, et assure la circulation des services bancaires avec une grande efficacité.

L'objectif de ce mémoire concerne la conception et la réalisation d'une solution Multi-Communications pour la gestion de CCP.

Trois solutions ont été proposées dans ce mémoire : Un site web (E-Banking), Une application J2ME (M-Banking) et un service de SMS Banking, ce qui donne aux clients la liberté de consulter leurs comptes et faire quelques autres opérations bancaires, par le service qui leur convient.

***Mots clés**: E-banking, M-Banking, SMS Banking, J2ME, PHP, PYTHON.*

Abstract:

The explosion in the number of mobile devices in the world to exceed that of computers is an important economic fact. With new telecommunications networks and the increase in the processing capabilities of the terminals, new opportunities to interact and communicate with customers, including via the Internet, made their appearance. Thus, the Mobile Internet brings opportunities for the expansion of the range of services offered by banks.
The improvement of these electronic techniques of the banking system was designed to cope with the challenges of the modern era, and ensure the movement of banking services with high efficiency.

The objective of this thesis concerns the design and implementation of a Multi-Communications solution for the management of CCP.

Three solutions have been proposed in this submission: web site (E- Banking), a J2ME (M-Banking) application and SMS Banking service, which gives customers the freedom to check their accounts and do a few other banking service that suits them.

***Key words**: E-banking, M-Banking, SMS Banking, J2ME, PHP, PYTHON.*

ملخص:

إن ازدياد عدد أجهزة الهاتف النقال وتجاوزها رقم أجهزة الكمبيوتر لحقيقة اقتصادية هامة، ومع تطور الشبكات الجديدة والزيادة في قدرة تخزين الأجهزة تم إيجاد طرق جديدة للتواصل مع الزبائن بما في ذلك استعمال شبكة الأنترنت والأنترنت للهاتف النقال ما جلب فرصا لتوسيع نطاق الخدمات المصرفية.

الهدف من تطوير هذه التقنيات هو مواكبة العصر وضمان أقصى حد من الخدمة.

والهدف من هذه الأطروحة هو تصميم وتنفيذ حل متعدد الاتصالات لإدارة الحساب الجاري (CCP)

وقد اقترحنا ثلاثة حلول: موقع الكتروني وتطبيق للهاتف النقال J2ME وخدمة "الرسائل القصيرة"، مما يتيح للعملاء حرية التحقق من حساباتهم بالخدمة الذي تناسبهم