La solution de sécurité WAP pour M-commerce

Salah Euschi[1], Hmida Djediai[2] et Azzedine Bilami [3]
1 Etudiant Edrsim, Université de Kasdi Merbah Ouragla, seuschi@yahoo.fr
2 Etudiant Edrsim, Université de Kasdi Merbah Ouragla, n_djediai@yahoo.fr
3 Maitre de conférences, Université de Batna, abilami@yahoo.fr

Résumé:

Le m-commerce est un sujet en développement. Il offre encore des opportunités pour des recherches et des applications futures. L'utilisation des réseaux et des dispositifs mobiles sans fil est en croissance. Nous assistons à un grand changement dans la réalisation des transactions commerciales. Avec l'émergence du commerce électronique, les chercheurs, les sociétés et les hommes d'affaires se focalisent sur la conduite des transactions en ligne. L'amélioration des technologies sans fil et mobiles facilite l'extension du e-commerce du réseau filaire au réseau sans fil.

Le succès important du téléphone mobile a transformé l'internet et le e-commerce. Le téléphone mobile qui est devenu un dispositif personnel de confiance PTD sera capable de gérer la sécurité des transactions commerciales dans le monde sans fil. Le protocole d'application sans fil WAP proposé par le forum WAP, est approprié pour sécuriser les services et les applications e-commerce.

Nous présentons dans ce papier un aperçu des environnements PKI et WAP et leur relation avec Internet. Nous étudions les standards de sécurité spécifiés pour le protocole WAP et comment ils ont été adaptés avec la technologie WPKI pour assurer les conditions de sécurité de M-Commerce. Nous présentons aussi quelques imperfections du WAP et comment ces problèmes peuvent être surmontés. Nous montrons l'impact des développements récents sur les opérateurs de réseaux, les fabricants des dispositifs mobiles et les utilisateurs.

Mots clés *: WAP, WPKI, WTLS, WML, WIM, cryptographie, mobile, sans fil*

1. Introduction

Le m-commerce peut être vu comme un sous ensemble du e-commerce, il désigne toute transaction monétaire pouvant être conduite via un réseau mobile. La communication sans fil s'est développée rapidement essentiellement dans le monde des transactions B2C (Business to Consumer) et avec l'utilisation large des dispositifs mobiles. La sécurité de m-commerce sera fondamentale pour étendre la fonctionnalité des téléphones mobiles. Actuellement, il y'a deux solutions pour sécuriser m-commerce : le i-mode, et le WAP. Le i-mode est une solution de communication sans fil, développé par NTTDoCoMo du Japan. Il utilise le langage HTML Compact (CHTML ou iHTML) pour la livraison de contenu et une commutation de paquets. Le i-mode a réalisé un succès énorme au Japan, mais il est la propriété de NTTDoCoMo, et nous nous disposons pas d'informations détaillées de ses solutions de sécurité, et ses procédures d'authentification et d'autorisation qu'il utilise avec son public [4].
Ce papier se concentre sur le WAP qui est actuellement la seule solution disponible publiquement pour la communication sans fil.

Avec l'utilisation de plus en plus répandue des applications sans fil, la face d'internet a rapidement changé. Les dispositifs mobiles commencent à dominer l'accès Internet par rapport aux PCs. Un argument fort en leur faveur est leur capacité de se connecter à Internet de n'importe quelle localisation et à n'importe quel moment. Ces dispositifs mobiles ne sont pas uniquement des outils pour la communication téléphonique sans fil, ils se sont transformés rapidement en PTDs (Personal Trusted Devices). Ce n'est pas le cas des PCs qui sont utilisés publiquement dans les entreprises et les autres organisations. Les dispositifs mobiles sont mois chers que les PCs et sont facilement portables par leurs propriétaires. Ils vont devenir l'outil dominant pour réaliser des transactions financières et autres activités relatives à m-commerce, par conséquent ils sont présents dans les applications m-commerce qui nécessitent des fonctions adéquates de sécurité [4].

Pour satisfaire les conditions de sécurité des communications sans fil, le forum WAP a spécifié la WPKI (Wireless Public Key Infrastructure). Le but des standards WAP est de fournir des services de données améliorés comme le contenu Internet et les transactions, aux dispositifs sans fil. La WPKI est une extension de la PKI aux environnements sans fil. Elle consiste en deux éléments de base : la

cryptographie à clé publique et le certificat numérique. La WPKI englobe la technologie cryptographique nécessaire et un ensemble de standards pour la gestion de sécurité de m-commerce.

Actuellement, les environnements sans fil ne sont pas complètement sécurisés. Aucun opérateur mobile ne peut garantir la sécurité de l'information transmise sur son réseau mobile. Il n'est pas possible aussi de vérifier l'identité de l'utilisateur d'un dispositif sans fil avec un processus d'authentification fiable. En d'autres termes, la confiance est inhérente aux dispositifs sans fil.

Dans ce papier nous présentons les méthodes de la cryptographie moderne (section 2), suivies par un aperçu de la PKI (section 3). Nous présentons le WAP1 et le WAP2 et comment le WAP2 a été amélioré pour surmonter les problèmes du WAP1 ? (section 4). Ensuite nous donnons les standards du WAP utilisés pour sécuriser les communications et les procédures d'authentification (section 5). Nous montrons les éléments d'amélioration de la WPKI par rapport à la PKI standard, et nous proposons notre solution de sécurité basée WAP qui considère la technologie existante et l'importance des transactions commerciales (section 6). Et enfin, dans la section 7, nous donnons quelques remarques en conclusion.

2. Les méthodes de cryptographie moderne

La cryptographie est la technologie qui permet de réaliser la communication d'information par le cryptage (ou le chiffrement).

a) Un scénario de base des crypto systèmes [6]

Alice et Bob souhaitent communiquer d'une manière secrète. On suppose que c'est Alice qui envoie un message à Bob. Le protocole cryptographique fondamental qu'ils emploient est un crypto système ou un chiffrement. Formellement Alice a un message M en texte clair, elle le chiffre en utilisant une fonction de cryptage e(.). Ce ci permet de créer un cryptogramme ou un texte chiffré : C = e(M). Elle envoie ce message à Bob. Ce dernier le décrypte avec une fonction de décryptage d(.) pour obtenir le message initial : d(C) = d(e(M)) = M.

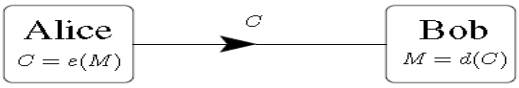

Fig.1. Un crypto système

b) Le système de cryptographie symétrique ou à clé privée

Alice et Bob partage une clé secrète K appelée aussi clé privée pour sécuriser la communication entre eux [6]. Les fonctions de cryptage/décryptage sont basées sur cette clé.

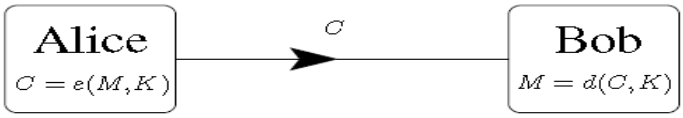

Fig.2. Un crypto système symétrique

Les algorithmes de cryptographie symétrique sont plus rapides et facilement implémentés sur le matériel. Se sont des opérations simples de substitution et de transposition.

Ces systèmes sont mieux adaptés pour une utilisation dans un environnement mobile sans fil, mais ils ne sont pas entièrement adéquats pour résoudre tous les problèmes de sécurité, et présentent les inconvénients suivants :

- Le principal inconvénient de ce crypto système provient de l'échange des clés secrètes pour des utilisateurs se trouvant dans des zones géographiques éloignées.
- Problème de gestion de clé : dans le e-commerce, le nombre de participants à la transaction est proportionnel au nombre de clés qu'ils doivent gérer. Pour n participants à la transaction, on aura besoin de ***n(n-1)/2*** clés privées enregistrés [7].

- Pas de support du mécanisme de non-repudiation: Les deux parties communicantes ont la même clé privée, il sera donc difficile de distinguer l'origine du chiffrement. Avec l'absence de ce mécanisme, ce système ne sécurise pas entièrement les environnements sans fil [7].

c) Le système de cryptographie à clé publique

Il permet de fournir la non-repudiation. Chaque utilisateur a une paire de clé, une pour le cryptage et l'autre pour le décryptage. La clé utilisée pour le décryptage est appelée clé privée, elle est gardée secrète et peut être associée à une fonction de hachage pour réaliser une signature numérique. La clé de cryptage, appelée clé publique peut être utilisée pour le cryptage et la vérification du propriétaire des signatures numériques. La clé publique est connue par tout le monde. La non-repudiation est assurée par l'utilisation de la signature numérique.

La réalisation des crypto systèmes non symétriques était l'évolution la plus importante dans la cryptographie moderne. Dans ce type de crypto systèmes à clé publique, Alice ne connait pas la clé privée de Bob [6].

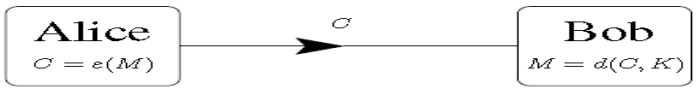

Fig. 3. Un crypto système à clé publique

Le principe des systèmes de cryptographie à clé publique est basé sur des problèmes mathématiques complexes (factorisation de nombre plus large, résolution de logarithme discret). Leur implémentation sur dispositif mobile est plus délicate. Pour remédier à cette situation, les applications utilisent un algorithme symétrique pour crypter le message, et un algorithme asymétrique pour crypter la clé. Cette méthode mixte (hybride) est plus efficace et mieux appropriée aux environnement sans fil [7].

3. Un aperçu de la PKI

La PKI (Public Key Infrastructure) est un ensemble de règles, de processus, de logiciels, de matériels et des technologies qui utilisent la cryptographie à clé publique et la gestion de certificat pour garantir la sécurité de la communication. La PKI a des services de confiance qui permettent le transfert sécurisé de l'information et supportent une grande variété d'applications m-commerce [4].

Le groupe de travail sur Internet X.509 PKIX définit une PKI comme suit :

« *The set of hardware, software, people and procedures needed to create, store, distribute and revoke certificates based on public key cryptography* » [4].

Pour fournir la sécurité des applications m-commerce, une PKI doit assurer les règles suivantes [3,4] :

- ***La confidentialité*** : la communication entre les deux parties doit être secrète. La confidentialité est réalisée par des techniques de cryptographie.
- ***L'intégrité*** : il faut s'assurer que les données transmises n'ont pas été modifiées ou altérées. L'intégrité est assurée par une signature numérique.
- ***L'authentification*** : un processus fiable qui permet d'identifier les identités des parties impliquées dans la communication. La signature numérique permet aussi de réaliser l'authentification.
- ***La non-répudiation*** : il faut s'assurer que les accords constituent un engagement légal qui ne peut être renié, en d'autres termes il doit être impossible pour des parties communicantes de nier ou de fausser les signatures numériques et les accords. La cryptographie à clé publique avec un certificat et une signature numérique assurent la non-répudiation.

Une PKI utilise des signatures numériques et des certificats basés sur une cryptographie asymétrique comme les algorithmes RSA et ECC-Elliptic Curves Cryptography. Le chiffrement asymétrique nécessite une paire de clés cryptographiques dont une est publique et peut être affichée dans un répertoire, l'autre

est privée et ne peut être révélée à personne. L'avantage principal d'une PKI est qu'elle permet de garantir le statut légal des accords signés numériquement.

La cryptographie à clé publique consiste à un calcul mathématique complexe pour déterminer la clé privée d'une clé publique donnée. La paire de clé publique/privée peut être utilisée pour réaliser des opérations mathématiques comme « cryptage/décryptage » ou « signature – vérification de signature » [4] .

Initialement, la cryptographie à clé publique est apparue comme un système idéal ne nécessitant pas un canal sécurisé. Mais, ce n'est pas le cas. Par exemple un adversaire usurpant l'identité de Bob peut donner sa clé publique à Alice qu'elle suppose qu'il s'agit de celle de Bob. L'adversaire intercepte le message chiffré de Alice à Bob, le décrypte avec sa propre clé privée, le ré-chiffre avec la clé publique de Bob et l'envoie à Bob. Donc il est nécessaire d'authentifier les clés publiques pour réaliser l'authenticité de l'origine des données chiffrées par les clés publiques elles mêmes. Une PKI utilise la gestion de certificat pour surmonter ce problème [4].

Un certificat numérique est un moyen pour associer sans ambigüité un support à une clé publique. L'idée de certificat numérique est simple : un organisme externe jouant le rôle d'une tierce partie de confiance (TTP-Trusted Third Party) appelée généralement une autorité de certification CA (Certification Authorities) tient des données personnelles et la clé publique dans un package qui est ensuite signé par la clé privée de la CA. Ainsi on peut utiliser la clé publique de l'autre partie seulement si la signature de certificat est vérifiée avec succès. Donc quelqu'un qui reçoit un message signé d'une partie pourra sans risque supposer qu'il a été envoyé par cette partie [4].

Une PKI consiste aux composants suivants [3,4] :

- *Les autorités de certification (CAs – Certificate Authorities)* : elles sont responsables de la publication et la révocation des certificats.
- *Les autorités d'enregistrement (RAs – Registration Authorities) :* elles vérifient le lien entre les clés publiques et les identités de leurs détendeurs (supports).
- *Les détendeurs de certificats (Certificate Holders)* : des personnes, des machines ou des agents logiciels qui ont été publiés avec les certificats et qui peuvent les utiliser pour signer numériquement des documents (les supports des certificats).
- *Les clients* : ils valident les signatures numériques et leurs chemins de certificat d'une clé publique connue d'une CA de confiance.
- *Les répertoires (Repositories)* : ils stockent les certificats, les listes de révocation de certificat et les rendent disponibles.

Une PKI réalise les fonctions suivantes [4]:

- *Enregistrement* : la CA vérifie que les informations fournies par le support sont correctes avant de publier un certificat.
- *Certification* : la CA publie un certificat qui contient la clé publique du support, délivre ce certificat au support et le publie dans les répertoires appropriés
- *Génération de clé* : dans certains cas, le support produit une paie de clés dans son environnement local, avant de passer la clé publique à la CA pour certification. Si la CA génère la paire de clés, les clés générées devront être fournies au support sous forme d'un fichier crypté ou un module matériel (tel qu'une carte SIM ou WIM).
- *Mise à jour de clé* : toutes les paires de clés et leurs certificats devront être mise à jour à des intervalles réguliers.
- *Révocation* : dans la majorité des cas, un certificat est considéré valide jusqu'à l'expiration de sa période de validité, mais il ya des scénarios qui nécessitent la révocation de la validité du certificat.
- *Inter-certification (Cross-certification)* : ce processus permet aux utilisateurs dans un domaine d'administration de vérifier des certificats publiés dans un autre domaine d'administration différent. Il permet l'interopérabilité des PKI de différents secteurs.

La PKI utilise le standard de certificat numérique X.509. Une fois un certificat est obtenu, la clé publique sera disponible par sa publication dans un répertoire de certificats d'une CA dans laquelle elle est stockée. Pour accéder aux répertoires de CA contenant les certificats X .509 et les CRLs (Certification Revocation

Lists), on utilise un protocole standard comme LDAP (Lightweight Directory Access Protocol). Pour vérifier la validité ou la révocation d'un certificat, nous avons deux mécanismes : la CRL d'une CA ou le protocole OCSP (Online Certificate Status Protocol).

Comparaison CRL et OCSP [3,4] : Les certificats révoqués par une CA sont placés dans une CRL qui contient les n° de série des certificats révoqués. La CA rend la CRL disponible en la plaçant dans un emplacement donné tel qu'un serveur X.500. Mais la méthode de vérification dans les CRLS présente des inconvénients :

- Pour vérifier si un certificat est dans une CRL, On rechercher la CRL entière dans le répertoire et la parcourir pour rechercher le n° de série du certificat en question. Si la CRL contient des milliers de certificats révoqués, la recherche est alors inefficace en délai.
- En plus, il y'a généralement un retard entre le temps de révocation du certificat et le temps de son enregistrement dans la CRL.
- Un autre problème est la gestion cohérente des réplications (des copies) des listes CRLs. Il faut s'assurer que toutes les copies sur les différents serveurs sont cohérentes.

Pour remédier aux inconvénients précédents, les deux contraintes suivantes doivent être vérifiées :

- La possibilité de demander juste le statut de révocation de certificat en question.
- Réduire considérablement le retard entre les moments de la révocation et de la publication de la révocation.

Le protocole OCSP - qui est un protocole automatique en ligne de vérification efficace du statut d'un certificat – prend en charge ces deux contraintes en fournissant un mécanisme qui permet de demander le statut d'un certificat particulier et d'obtenir cette information d'une façon plus opportune. Le temps de réponse est important particulièrement dans de grands transferts de fonds ou le commerce d'actions (la bourse). Un client OCSP publie une demande de statut d'un certificat à un répondeur OCSP, et suspend l'acceptation du certificat jusqu'à ce que le répondeur reconnaisse la validité de ce certificat.

4. L'environnement WAP (Wireless Application Protocol)

Le forum WAP définit le WAP comme suit [3,4]:

« *WAP is an open global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly* ».

Le WAP est un espace ouvert et interopérable pour la diffusion du contenu Internet et applications aux dispositifs mobiles. Les dispositifs WAP peuvent accéder à des services interactifs tels que l'information, les services basés localisation, et les jeux interactifs. Le WAP s'utilise sur plusieurs dispositifs portables comme les PTDs, et les téléphones mobiles Bluetooth [4].

La meilleure analogie de l'environnement WAP est le Web. Le Web consiste en trois principaux composants : un client Web, un réseau IP et un serveur Web. Les clients utilisent un navigateur sur un PC connecté au serveur Web pour communiquer sur le réseau IP, le serveur Web fournit l'information sous forme de pages écrites en langage HTML.

Fig. 4 – Les composants de l'environnement Web (Source : certicom)

Il y a des différences entre les environnements WAP et Web [13]:

- Les dispositifs sans fil de l'utilisateur final ont moins de puissance de calcul comparés aux PCs utilisés sur le Web. Les dispositifs sans fil ont des ressources limitées : des CPUs moins puissants, moins de mémoire, moins de capacité de stockage de données et de programmes, une bande passante moins large et des petits affichages).

- Le WAP utilise le WML (Wireless Markup Language) au lieu du HTML. Les pages WML (ou les formulaires WML) sont plus petites que celles du HTML, ce qui signifie qu'un contenu particulier est crée spécialement pour les dispositifs WAP.
- Les programmes dans l'environnement WAP doivent être optimisés et efficaces. Ils consomment moins de mémoire et nécessitent un minimum de cycles CPU. Les dispositifs sans fil étant limités en calcul CPU et en capacité de stockage. les objets de données et de transactions doivent être compacts avec un minimum de taille de stockage, de mémoire et de cycles de calcul CPU.
- Les protocoles WAP et Web (http, ftp…) ne sont pas directement interopérables, un composant appelé passerelle WAP (WAP Gateway) est nécessaire pour transformer les protocoles Web en WAP et vice versa. Cependant le protocole récent WAP2 a été amélioré, il intègre le protocole IP de l'internet et fournit une sécurité de bout en bout en utilisant le protocole de transport TLS/SSL , de dispositifs mobiles aux serveurs de contenu (voir fig. 5).

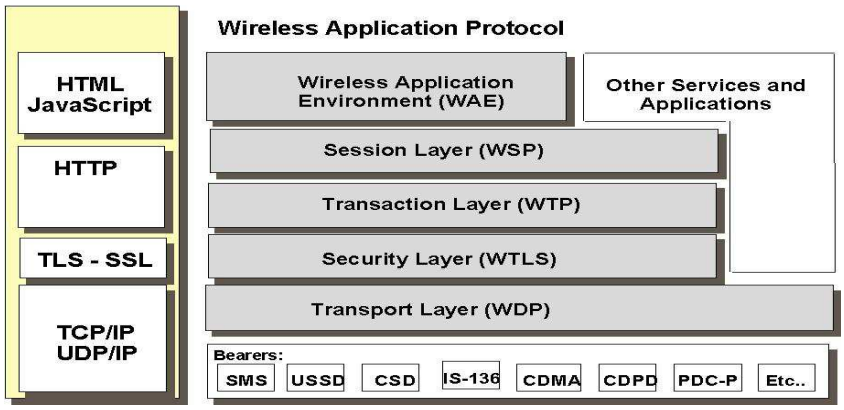

Fig. 5 – Le WAP vs le protocole Internet IP . (Source: Forum WAP)

Du sans fil à Internet

L'environnement internet WAP consiste à un client WAP, un réseau sans fil, une passerelle WAP (ou un proxy WAP), un réseau filaire IP, et un serveur de contenu Web. Le client WAP communique avec la passerelle WAP avec des données WML transmises sur un réseau sans fil. La passerelle WAP traduit les données WML en HTML et vice versa, transmet les données entre les réseaux sans fil et filaire et communique avec le serveur Web (voir fig. 6) [13].

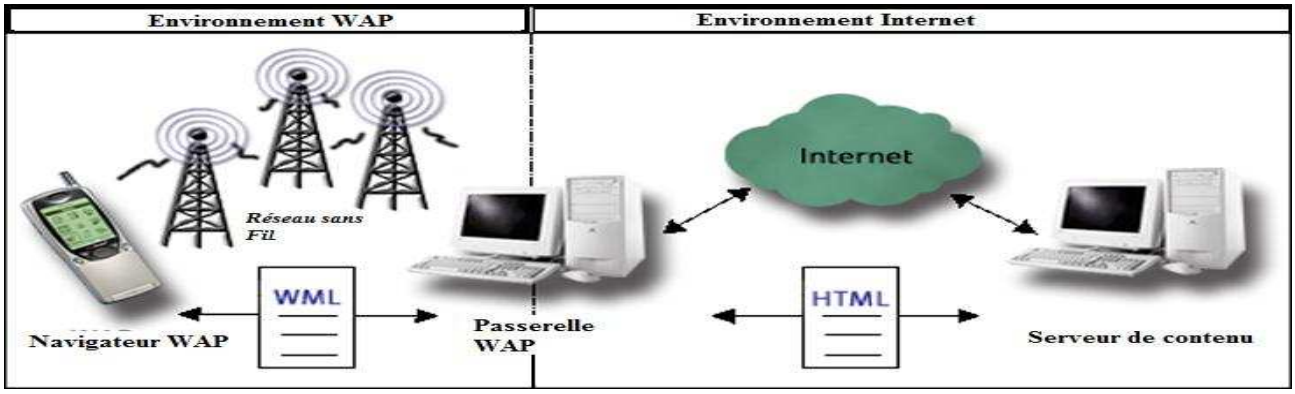

Fig. 6 – les composants de l'environnement internet WAP (Source: certicom)

La version WAP2 permet d'étendre l'internet à l'environnement sans fil. Elle inclut la technologie GPRS (2 .5 G) et les générations de bande passante 3G et 4G (avec des services de paquets ajoutés). Le WAP2 fournit des protocoles tels que TCP, et http, ce qui permet à un dispositif sans fil d'utiliser la technologie Internet existante. Le navigateur WAP utilise le langage WML2 basé sur XHTML. Le XHTML est un langage développé par le consortium W3C pour remplacer et améliorer le HTML classique. C'est un langage proche de XML et permet d'utiliser les nouvelles technologies de l'Internet. Le WML2 est entièrement conforme au XML [5].

Les autres améliorations du WAP2 concernent des applications et des services permettant d'étendre les capacités des dispositifs mobiles. Parmi ces services, nous pouvons citer : WAP push, User Agent Profile, synchronisation de données, Multimedia Messaging Services (MMS),… [5].

5. La sécurité WAP

Le forum WAP a standardisé un protocole de sécurité de couche transport (WTLS- Wireless Transport Layer Security) faisant partie de la pile WAP1. WTLS fournit une sécurité de transport entre un dispositif WAP et une passerelle WAP qui réalise la transformation du protocole en SSL/TLS. WTLS est le protocole de sécurité sans fil équivalent au protocole TLS/SSL largement utilisé sur Internet. Malheureusement, il n'y a pas de sécurité de bout en bout et la passerelle WAP doit être placée dans un domaine de confiance [1,8].

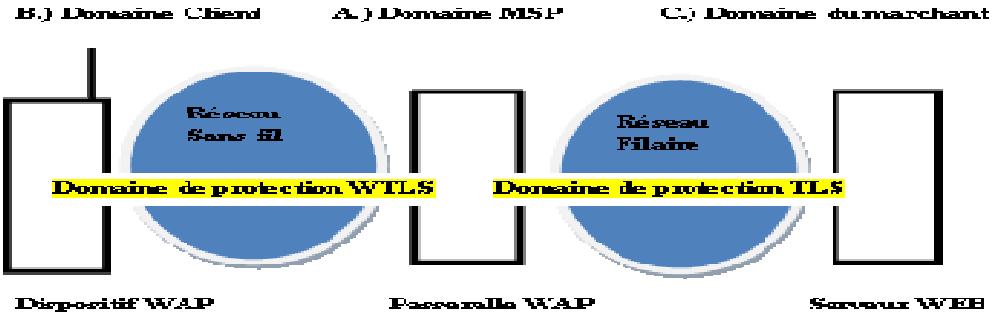

Figure 7. Les trois parties impliquées dans une transaction type m-commerce utilisant le WAP: (A). La compagnie de téléphone mobile (The mobile service provider, MSP) utilise la passerelle WAP pour se connecter entre les réseaux filaire et sans fil. (B). Le client utilise un téléphone mobile WAP. (C). Le site Web du marchand est connecté au réseau filaire. Les réseaux illustrés, le premier est généralement sans fil, un réseau d'accès mobile, le second est fixe, généralement c'est l'internet filaire [8].

Le problème de sécurité de la passerelle WAP : La passerelle WAP a pour mission de convertir des informations provenant de l'Internet au format WAP, codant et décodant les requêtes et les réponses entre le dispositif WAP et le serveur web. La passerelle peut se situer chez un opérateur téléphonique, un fournisseur d'accès indépendant ou au sein de l'entreprise. La sécurité n'étant pas fournie de bout en bout, la passerelle WAP peut être compromise au moment de la conversion des messages du protocole WTLS au protocole TLS/SSL. Dans le processus de conversion, les données sont mises en texte clair et ensuite recryptées. La passerelle peut être compromise lorsque les données seront en texte clair, ce qui met en péril la session sécurisée [3,4,8].

Le WAP2 surmonte ce problème par des sessions sécurisées avec TLS/SSL de bout en bout [1]. Il utilise le *TLS Tunneling* pour assurer la sécurité d'échange du client au serveur Web. En plus, le WAP2 inclut un support de sécurité niveau application comme la signature numérique du texte [9].

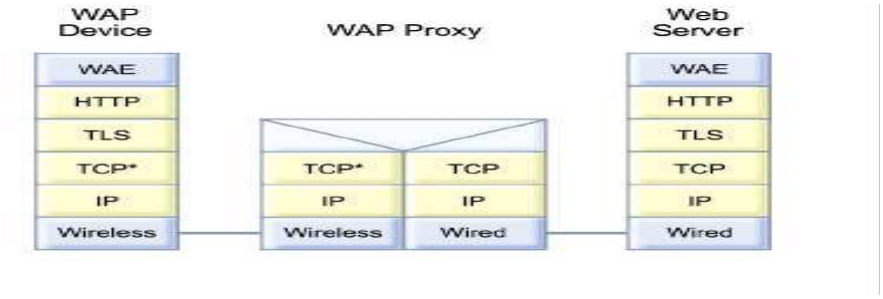

Figure 8. Support de l'architecture WAP2 pour TLS Tunneling. (Source: Forum WAP)

La figure 8 montre un proxy WAP2. Il est placé entre les réseaux sans fil et les réseaux filaires pour améliorer la performance par l'utilisation des protocoles WP-TCP (TCP*) et WP-HTTP. Ces versions de protocoles sans fil sont interopérables avec TCP et http [11].

Le WAP utilise plusieurs standards pour appliquer la sécurité au niveau application, transport et gestion dans l'environnement sans fil. Ces standards sont :

- WIM – Wireless Identity Module : une puce matérielle qui réside optionnellement dans le dispositif WAP (téléphones mobiles et PTDs). Cette puce peut stocker une clé matérielle comme la clé publique PKI et la clé privée de l'utilisateur. Une puce WIM a une mémoire pour stocker des données et des programmes. Elle peut être sur un slot séparé ou sur le même slot de la carte SIM (carte SWIM : SIM et WIM sur le même slot) [3,4,13].

  Au niveau de la couche de sécurité transport, le WIM est utilisé pour les buts suivants [10]:

  - Exécuter les opérations cryptographiques durant le dialogue, particulièrement celles qui sont utilisées pour l'authentification du client.
  - Protéger les sessions WTLS sécurisées par des clés de session générées par le WIM.
  - Le WIM utilise les clés publiques/privés stockées pour réaliser des opérations de signature (eg, ECDSA or RSA) pour l'authentification du client et pour l'échange de clé (eg, ECDH key, in ECDH_ECDSA handshake).

  Les opérations de niveau sécurité application utilisant le WIM comprennent la signature, la vérification de signature et le déchiffrement de clé. Toutes ces opérations utilisent une clé privée stockée dans le WIM. Le déchiffrement de clé est utilisé lorsqu'une application reçoit un message avec une clé chiffrée à l'aide d'une clé publique qui correspond à une clé privée dans le WIM. Le dispositif mobile envoie la clé au WIM, qu'il la décrypte en utilisant la clé privée et retourne la clé déchiffrée. Le dispositif mobile utilise alors cette clé pour décrypter le message attaché [10].

- WMLSCrypt (WML Script Crypto API) : Une API qui permet l'accès à des fonctions de sécurité dans une librairie WMLSCLib (WML Scrypt Crypto Library). Elle permet à l'application WAP d'utiliser les objets et des services de sécurité gérés par d'autres standards autre que le WAP. Les fonctions de base dans WMLSCrypt et WMLSCLib comprennent : générer des paires de clés, stocker les clés et autres données personnelles, contrôler l'accès aux clés et aux données stockées, générer et vérifier les signatures numériques, crypter et décrypter les données. WML Script peut utiliser un module WIM intégré pour fournir les fonctions de cryptographie [4]. Pour plus détails, on peut se réfèrer à [11].

- WTLS/TLS : protocole de sécurité niveau transport basé sur le protocole de sécurité Internet connu sous le nom de TLS ou SSL. Le WAP2 avec WP-TCP utilise TLS au lieu de WTLS pour surmonter le problème de sécurité de la passerelle WAP, et assure une sécurité de bout en bout au niveau transport (TLS tunneling). Cependant, un problème majeur de performances se pose, a cause du temps pris par les calculs cryptographiques et la charge protocolaire du TLS.

  WTLS /TLS permet de réaliser les règles de sécurité : authentification, confidentialité et intégrité. L'authentification est réalisée par la signature numérique et un certificat PKI à clé publique, la confidentialité par le cryptage des données, et l'intégrité par l'emploi du hachage de données et la protection de DOS (Deni Of Service) par le protocole TLS qui détecte et rejette les données altérées ou non vérifiées [4,13].

  Trois niveaux d'authentification avec WTLS [3]: Classe I - Pas d'authentification, classe II : Authentification uniquement du serveur, classe III : Authentification du client et du serveur. La non-répudiation est fournie par un certificat WPKI qui peut être un certificat CA à clé publique utilisé pour WTLS classe 2, un certificat client à clé publique utilisé pour WTLS classe 3, ou un certificat client à clé publique utilisé conjointement avec la fonction Crypto.signText de WMLScript [12].

- WP-TCP (Wireless profiled TCP) : Il est optimisé pour les environnements sans fil et complètement interopérable avec le standard TCP de l'internet [5].

- WPKI (Wireless Application PKI) [12] : elle n'est pas une nouvelle PKI, mais une extension optimisé de la traditionnelle PKI pour l'environnement sans fil. WPKI et PKI renforcent les règles de transactions m-commerce et gèrent la relation entre les parties communicantes, les clés et les certificats. La WPKI permet d'étendre le e-commerce aux environnements sans fil et mobiles. Elle sécurise le commerce électronique dans l'environnement sans fil au niveau transport par WTLS/TLS et au niveau application par WMLSCrypt et WIM. Dans lés réseaux filaires les standards PKI de l'IEFT sont les plus utilisés. Dans les réseaux sans fil, les standards WPKI du Forum WAP sont les

plus utilisés. La WPKI étant une extension de la PKI, elle est entièrement interopérable avec la PKI [3,4,13].

6. La WPKI : Wireless Public Key Infrastructure

6.1 Un aperçu de la WPKI

Le principe fondamental de la PKI n'a pas changé dans les environnements sans fil. L'accès à un dispositif PTD à travers l'interface radio, pose certains défis. Les PTDs ont généralement des ressources limitées avec une bande passante plus faible. Le protocole TCP/IP et les services PKI sont des solutions qui nécessitent un calcul plus intensif. Ces solutions ne sont pas donc appropriées aux environnements sans fil. A l'exception de ces problèmes, les éléments de base de la PKI et le certificat sont les mêmes [3,4].

Les solutions WPKI utilisent des agents réseau pour s'occuper de certaines taches. Les dispositifs mobiles ont des ressources limitées, ils doivent être au minimum capables de réaliser la fonction de signature numérique pour établir la WPKI. Les agents réseau peuvent exécuter toutes les autres tâches comme la validation, l'archivage et la livraison de certificat. Les clés privées peuvent être stockées dans le serveur proxy ou dans les WIM/SWIM des PTDs. Malheureusement la solution WIM/SWIM exige plus de performance pour générer des paires de clés par l'utilisateur final [4].

Le manque de standards est une barrière pour le développement de la WPKI. L'établissement de la confiance dans une WPKI est crucial pour le succès des applications m-commerce exploitant les opportunités offertes par les PTDs. Cette confiance est obtenue par une technologie fiable et un cadre légal basé sur une législation internationale de la PKI. Les problèmes d'anonymats, la vie privée, le contrôle des gouvernements, les règles d'industrie et les standards représentent des chalenges qu'il faut faire face [3,4].

Un utilisateur final non encore enregistré avec PKI et tente de se connecter à un fournisseur de service ou un serveur de contenu. Le fournisseur de service exige des signatures numériques sur ses transactions et sécurise ses communications, il notifie l'utilisateur qu'il doit contacter un portail PKI en lui fournissant son identification (PKI ID) comme l'URL, le nom de l'autorité de certification (CA) etc. [4,13].

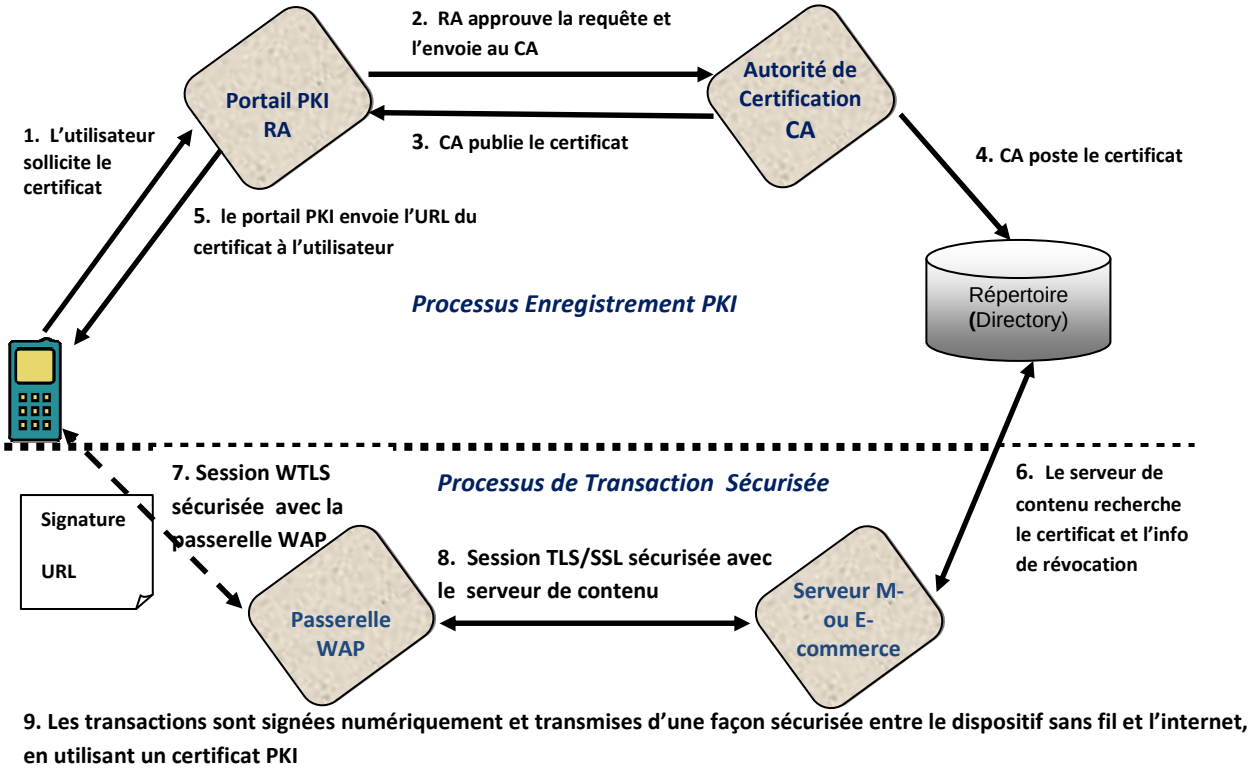

Fig.9. les processus d'enregistrement et la sécurité de la transaction avec WPKI

La WPKI nécessite les mêmes composants utilisés dans la PKI traditionnelle : l'application de l'utilisateur final (EE- End-Entity Application), la CA, la RA et le répertoire PKI. Mais la EE et la RA

sont implémentées différemment, et un nouveau composant comme le portail PKI est aussi nécessaire [13].
L'application WPKI sur dispositif mobile WAP est implémentée comme un programme optimisé. Elle utilise l'API WMLSCrypt pour les services de clés et les opérations de cryptographie comme dans le cas de la PKI traditionnelle.
Le Portail PKI est un serveur de réseau, comme le proxy WAP, il fonctionne logiquement comme une autorité d'enregistrement (RA) et il est responsable de traduire des demandes faites par le client WAP à la RA et à la CA dans la PKI. Le Portail PKI intègre les fonctions de la RA et interagit avec les dispositifs WAP sur le réseau sans fil et avec la CA sur le réseau filaire (voir fig. 9) [4,13].

6.2 Les améliorations de la WPKI

La WPKI est une optimisation des standards de la traditionnelle PKIX de l'IETF pour les environnements sans fil. Elle a optimisé en particulier les protocoles PKI, le format de certificat comme les clés et les algorithmes cryptographiques. Nous donnons plus de détails sur ces améliorations [3,4,7,13]:

- ***Les protocoles WPKI*** : La méthode de gestion des demandes de service PKI utilise les formats du codage BER/ DER du standard ASN.1 qui exigent plus de ressources de calcul dépassant les limites des dispositifs WAP. Les protocoles WPKI sont implémentés en utilisant WML2 et l'API WMLSCrypt. WML et la fonction signText dans WMLSCrypt fournissent une économie significative dans le chiffrement et la gestion des services PKI comparée aux méthodes utilisées dans la PKI.

- ***Le format de certificat WPKI*** : il consiste à réduire le volume du stockage pour un certificat à clé publique. Un nouveau format ((WTLS Certificate format) pour les certificats coté serveur, a une taille plus réduite comparé à celui du certificat standard X.509 utilisé sur l'internet filaire. Une autre réduction significative dans le certificat WPKI est l'utilisation de la cryptographie à courbe elliptique ECC (Elliptic Curve Cryptography). Avec les algorithmes ECC, l'économie dans le volume de stockage du certificat est plus de 100 octets en raison des clés ECC plus petites par rapport à d'autres schémas de signature. Comme le format de certificat WPKI est un sous profile du format PKI, la WPKI restera interopérable avec la PKI.
- ***Les algorithmes de cryptographie et les clés WPKI :*** Les algorithmes ECC sont reconnus comme les plus optimisées et donc les meilleurs pour supporter la sécurité dans l'environnement sans fil. Les clés ECC pour signatures numériques sont six fois moins que celles des autres schémas de signatures (164 bits ECC vs 1024 bits RSA). Ceci permet une optimisation dans le stockage de clé, la taille du certificat, l'utilisation de la mémoire et le calcul des signatures numériques. La technologie ECC est complètement supportée par les standards de sécurité WAP et largement acceptée par les fabricants des dispositifs WAP.
  Une mesure de temps réalisé sur le dispositif mobile Palm VII a montré que le temps d'exécution de la cryptographie pour une authentification mutuelle *WTLS handshakes* basée ECC 163 bits est plus rapide de plus de 6 fois que celui d'une authentification mutuelle *WTLS handshakes* basée RSA 1024 bits [2].

6.3 Notre Proposition pour l'implémentation de la sécurité pour un système m-commerce utilisant la technologie WAP

Notre solution doit avoir le niveau de sécurité le plus élevé et qui correspond au WTLS classe 3 (authentification mutuelle avec un certificat WPKI, les clés publiques de la CA doivent être fournies au client et au serveur). Le chiffrement de données utilise un crypto-système asymétrique. La sécurité est implémenté au niveau couche application, les deux fonctions *SignText* et *EncryptText* de WMLSCript via l'utilisation du module WIM, permettent respectivement d'authentifier le client auprès du serveur final et chiffrer les données afin de s'assurer de leur intégrité. Ce niveau élevé de sécurité peut être associé à des transactions importantes (comme le macro paiement). Il suppose que le dispositif mobile intègre entièrement la technologie WAP2 et peut stocker les clés publiques/privées. Le protocole proposé doit réaliser la sécurité de la transaction de bout en bout, il permet de :

- établir une authentification mutuelle entre le client et le serveur
- chiffrer les données transmises pour qu'elles ne soient pas visibles par la passerelle
- signer numériquement la transaction pour assurer leur intégrité. La signature numérique et sa vérification seront basées sur la cryptographie ECC, pour vérifier plus rapidement l'identité des deux parties.

Pou réduire la charge cryptographique du côté mobile, nous intégrons un serveur de sécurité comme un tiers de confiance (TTP), et qui peut être implémenté avec la passerelle WAP. Le TTP s'occupe de la grande charge cryptographique nécessaire pour vérifier la chaîne de certification et valider la révocation d'un certificat. Il permet à un client WAP de récupérer le certificat du serveur à connecter. Le TTP vérifie la validité du certificat ainsi que la chaîne de certification. Ensuite, il récupère la clé publique du certificat du serveur et l'envoie au client d'une manière authentifiée et protégée [7,14].

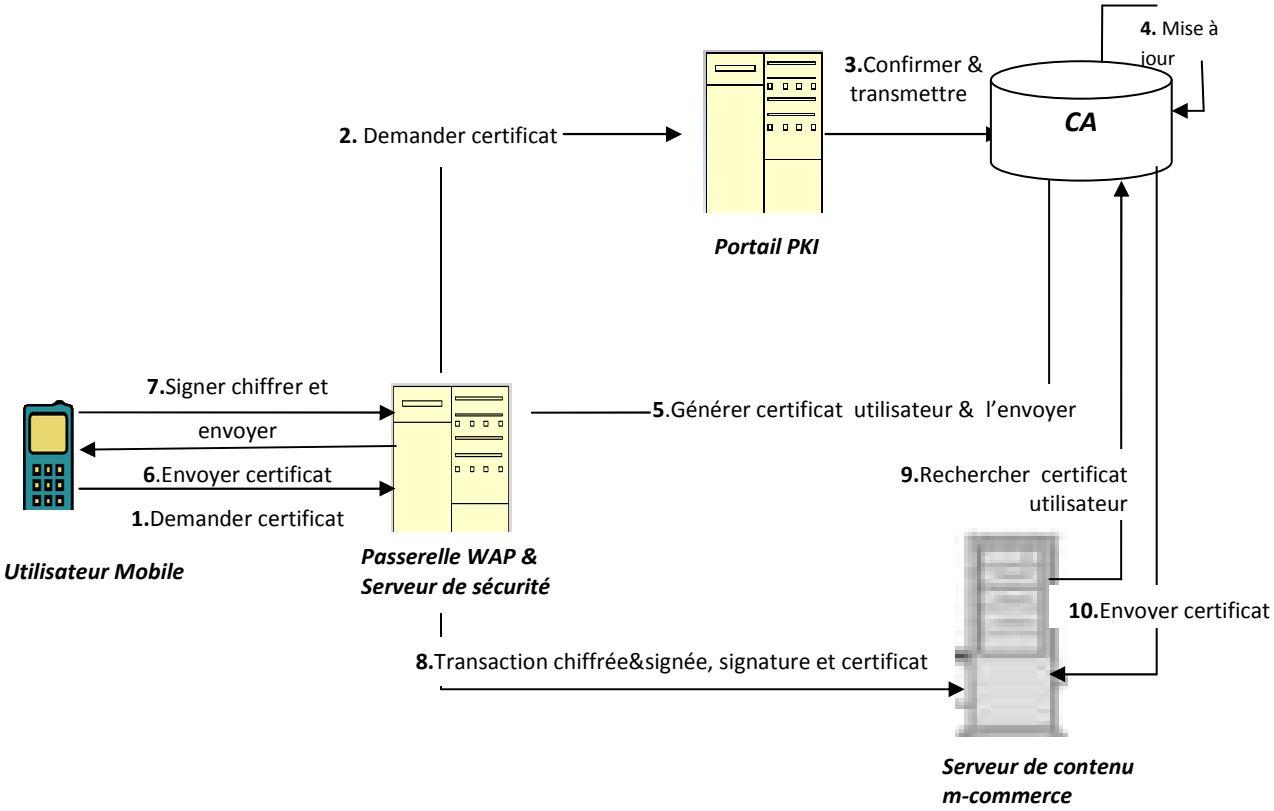

Fig.10. Protocole de sécurité niveau application basé WPKI des transactions mobiles

Nous proposons aussi d'autres protocoles avec des niveaux de sécurité moins élevés et pouvant être utilisés dans des transactions de moins importance (micro paiement et mini paiement).

Pour généraliser l'utilisation du système m-commerce, nous devons aussi considérer, dans notre solution de sécurité, les dispositifs mobiles n'intégrant pas le WAP et ne pouvant pas stocker les clés et réaliser des signatures numériques. Dans ce cas, le TTP peut réaliser à leur place la certification, l'authentification et la signature numérique après avoir reçu l'autorisation du client mobile. La communication entre le client mobile et le TTP, peut se faire par SMS (Short Message Service).

7. Conclusion

Les standards du WAP ont étendu le contenu Internet et les transactions aux dispositifs sans fil. Les conditions de sécurité e-commerce sont les mêmes dans l'environnement filaire et l'environnement sans fil et la PKI joue un rôle important pour satisfaire ces exigences. La WPKI est une extension à la traditionnelle PKI et comprend la plupart des concepts présents dans la PKI. Cependant, la WPKI doit être optimisée en utilisant une cryptographie plus efficace appropriée aux environnements sans fil comme

les algorithmes ECC. L'infrastructure de sécurité WPKI basée sur la cryptographie à clé publique et les signatures numériques permet d'assurer la confidentialité, l'intégrité des données de la transaction, l'authentification des parties impliquées, et la non-repudiation. Les PTDs doivent être capables de générer les signatures numériques et permettre à l'utilisateur de s'authentifier lui-même et à distance sur le réseau.

Les opérateurs de réseau mobile sont en face au défi d'assurer une authentification sécurisée et des services ajoutés entre les PTDs et les prestataires de service et de contenu. Ils assurent aussi les fonctions de cryptage/décryptage, la validation des certificats et la génération des clés.

Les fabricants des équipements mobiles seront aussi en face au défi de réaliser des dispositifs sans fil plus compacts, puissants et faciles à utiliser avec des mécanismes de sécurité employant la biométrie. Ces développements vont contribuer au succès de la WPKI. Les cartes SIM/SWIM sont des modules matériels sécurisés, ils stockent les clés cryptographiques et exécutent des fonctions de signatures numériques. Les dispositifs mobiles de la 3G devront contenir ces cartes [4] .

La spécification WAP continue à évoluer pour satisfaire les besoins du marché. Elle adapte des standards et des protocoles appropriés à l'environnement sans fil. Actuellement le WAP2 permet une meilleure intégration avec l'internet en utilisant les standards de l'internet TCP/IP et Mobile IP. Il surmonte le problème de sécurité dans la passerelle WAP en utilisant TLS sur tout le chemin du dispositif WAP au fournisseur de service m-commerce. WAP2 est aussi compatible avec la version précédente du WAP. Mais il ya des défis futurs [4] :

- Etablir la confiance dans la WPKI, car le succès des applications sans fil dépend de cette WPKI.
- Mettre en place une infrastructure pour fournir les services WPKI et qui seront accessibles à l'utilisateur final par quelques boutons de son dispositif, pour réaliser les solutions de sécurité.
- Enfin, une législation mondiale de la PKI est nécessaire pour généraliser m-commerce à travers le monde.

8. Références

[1] Scarlet Schwiderski-Groshe & Heiko Knospe, ***Secure M-Commerce***, University of London, T-Systems Nova GmbH, Germany, October 2002

[2] JVescio, ***Introduction to m-commerce***, Yodlee.com Inc., August 2000

[3] Chan Yeob Yeun & Tim Farnham, ***Secure M-Commerce with WPKI,*** Toshiba Telecommunication Research Laboratory, England, October 2001

[4] Chan Yeob Yeun, ***Secure M-Commerce with WPKI,*** Toshiba Telecommunication Research Laboratory, October 2001

[5] WAP Forum***, WAP 2.0 Technical White Paper***, version January 2002, http://www.wapforum.org/

[6] John TALBOT, Dominic WELSH, ***Complexity and Cryptography an Introduction***, Cambridge University Press, 2006

[7] W.-B. Lee, ***Wireless Security***, Feng Chia University, 100 Wen Hua Road, Taiwan, October 2006

[8] Niels Christian Juul and Niels Jørgensen, ***WAP may Stumble over the Gateway (Security in WAP-based Mobile Commerce)***, Department of Computer Science, Roskilde University, Denmark

[9] WAP Forum, ***Wireless Application Protocol Architecture Specification,*** Version 12-July-2001, http://www.wapforum.org/

[10] WAP Forum, ***Wireless Identity Module Part: Security,*** Version 12-July-2001, http://www.wapforum.org/

[11] WAP Forum, ***WMLScript Crypto Library,*** Version 20-Jun-2001, http://www.wapforum.org/

[12] WAP Forum, ***Wireless Application Protocol Public Key Infrastructu***re, Version 24-Apr-2001, http://www.wapforum.org/

[13] Certicom Office Locations**,** ***Wireless Public-Key Infrastructure*****,** Certicom Corporation 2001, http://www.certicom.com/

[14] JASEN MARKOVSKI, MARJAN GUŠEV**,** ***Application level security of mobile communications*****,** Ss. Cyril and Methodius University 2004