Un Protocole de Sécurité Niveau Application Basé WPKI pour les Transactions du Client Mobile

Salah Euschi
Université Hadj Lakhder Batna
euschi.salah@univ-ouargla.dz

Azeddine Bilami
Université Hadj Lakhder Batna, Laboratoire LaSTIC
abilami@yahoo.fr

Résumé—**Avec l'expansion du web, le commerce électronique a révolutionné le commerce traditionnel et a amélioré les ventes et l'échange des marchandises et d'informations. L'émergence des réseaux sans fil et mobiles a étendu le e-commerce à un nouveau domaine d'applications et de recherche appelé m-commerce, défini comme l'achat et la vente de produits, de services ou d'informations sur l'internet via l'utilisation des dispositifs mobiles portables.**

Cependant le futur du m-commerce ne peut être radieux que si l'échange d'informations entre les utilisateurs mobiles et les fournisseurs soit entièrement sécurisé. Le téléphone mobile est devenu un dispositif personnel de confiance PTD (Personal Trusted Device) et 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 m-commerce.

Ce papier donne un aperçu sur les environnements PKI et WAP et leurs relations avec Internet. Nous présentons les standards de sécurité spécifiés pour le protocole WAP et comment ils ont été adaptés avec la technologie WPKI pour assurer les exigences de sécurité du m-commerce. Nous présentons aussi quelques imperfections du WAP et comment peuvent- elles être surmontées ? Nous proposons enfin un protocole de sécurité au niveau application basé WPKI pour sécuriser les transactions du client mobile.

Mots clés : *WAP, WPKI, WTLS, WML, WIM, cryptographie, m-commerce, sans fil, dispositif mobile.*

I. INTRODUCTION

Le m-commerce peut être vu comme un sous ensemble de e-commerce, il désigne toute transaction monétaire pouvant être conduite via un réseau mobile. Avec l'utilisation répandue dispositifs mobiles, la communication sans fil s'est développée rapidement essentiellement dans le monde des transactions B2C (Business to Consumer). La sécurité de m-commerce sera fondamentale pour étendre la fonctionnalité des téléphones mobiles.

Ce papier se concentre sur la technologie WAP, qui est 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 se sont transformés rapidement en PTDs. Ils stockent des données personnelles (clés et certificats) pour envoyer ou recevoir des informations privées. Les dispositifs mobiles sont moins 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 [1].

Pour satisfaire les exigences de sécurité des communications sans fil, le forum WAP a spécifié la WPKI. Le but des standards WAP est de fournir des services de données améliorés comme le contenu Internet et les transactions, aux dispositifs sans fil. E-commerce et m-commerce ont leurs exigences spécifiques de sécurité. Ces exigences sont réalisées par des techniques de cryptographie et des services PKI. 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.

Le WAP Identity Module (WIM) est un module matériel sécurisé, il permet d'améliorer la sécurité de l'implémentation WTLS et certaines fonctions de la couche de l'environnement d'application sans fil (WAE). Il est utilisé particulièrement pour stocker et traiter les informations nécessaires pour l'authentification de l'utilisateur [2].

Dans ce papier nous présentons un aperçu de la PKI (section 2). Nous présentons le WAP1 et le WAP2 et comment le WAP2 a été amélioré pour surmonter les problèmes du WAP1? (section 3). Ensuite nous donnons les standards du WAP utilisés pour sécuriser les communications et les procédures d'authentification (section 4). Nous montrons les éléments d'amélioration de la WPKI par rapport à la PKI standard (section 5). Nous proposons notre solution de sécurité basée WPKI 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.

II. UN APERÇU DE LA PKI (PUBLIC KEY INFRASTRUCTURE)

Les services de sécurité de la cryptographie moderne tirent profil des avancées en technologie de calcul pour réaliser les objectifs de sécurité, les données numériques sont chiffrées et déchiffrées par des algorithmes cryptographiques, il ya deux types de systèmes : Le système à cryptographie symétrique basée sur une clé secrète partagée, et le système à cryptographie asymétrique ou à clé publique, basée sur une paire de clés, dont une est publique et l'autre est privée. La réalisation des crypto systèmes à clé publique était

l'évolution la plus importante dans la cryptographie moderne [3].

L'implémentation de la cryptographie à clé publique sur le dispositif mobile est délicate. Les clés pour les chiffrements symétriques comme AES doivent être échangées avec des crypto systèmes à clé publique forts comme RSA ou ECC. Les paires de clés ECC ont des tailles plus petites que celles de RSA et DSA/DH. Les crypto systèmes ECC permettent une meilleure performance en calcul CPU et en consommation d'énergie, aussi bien qu'une économie en mémoire et en bande passante. Ces caractéristiques les rendent particulièrement adaptés aux dispositifs mobiles limités en ressources.

Dans la cryptographie de courbe elliptique ECC, nous avons trois standards d'algorithmes : ECIES (Elliptic Curve Integrated Encryption Scheme), ECDSA (Elliptic Curve Digital Signature Algorithm) et ECDH (Elliptic Curve Diffie-Hellman) [4].

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 elle est utilisée dans un grand nombre d'applications e-commerce [1].

A. Les services de la PKI

Pour fournir la sécurité des applications m-commerce, une PKI doit assurer les services de confidentialité, d'intégrité, d'authentification et de non-répudiation.

Une PKI utilise des signatures numériques et des certificats basés sur une cryptographie asymétrique comme les algorithmes RSA et ECC. Un certificat numérique est un moyen pour associer sans ambigüité un support (une personne, une organisation, un matériel ou un logiciel) à une clé publique [1].

B. Les composants de la PKI

Une PKI consiste aux composants suivants [1,3] :

- *Les autorités de certification* (CAs – Certificate Authorities) pour publier et révoquer les certificats.
- *Les autorités d'enregistrement* (RAs – Registration Authorities) pour vérifier le lien entre les clés publiques et les identités de leurs détenteurs.
- *Les détenteurs* (ou supports) de certificats (Certificate Holders) : se sont 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 clients* pour vérifier les signatures numériques et leurs chemins de certificat à clé publique.
- *Les répertoires* (Repositories or Directories) pour stocker les certificats et les listes de révocation de certificats.

C. Les fonctions de la PKI

Une PKI réalise les fonctions suivantes [1,3] :

- *Enregistrement* du certificat par la CA.
- *Certification* ou publication du certificat par la CA.
- *Génération de paire de clés* par le support ou la CA.
- *Mise à jour de clés* à des intervalles de temps réguliers.
- *Révocation* des certificats expirés.
- *Cross-certification* pour assurer l'interopérabilité des PKI de différents secteurs.

III. L'ENVIRONNEMENT WAP (WIRELESS APPLICATION PROTOCOL)

Le WAP s'utilise sur plusieurs dispositifs portables comme les PTDs (PDAs et Smartphones), et les téléphones mobiles intégrant Bluetooth.

A. Comparaison Web et WAP

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.

Il y a des différences entre les environnements WAP et Web [1,5] :

- Les dispositifs sans fil de l'utilisateur final ont des ressources limitées.
- Le WAP utilise le WML (Wireless Markup Language) au lieu du HTML. Les pages WML sont plus petites que celles du HTML, ce qui signifie qu'un contenu particulier est crée spécialement pour les dispositifs WAP.
- Les programmes et les objets de données dans l'environnement WAP doivent être optimisés, ils consomment moins de mémoire et nécessitent un minimum de cycles CPU.
- Les protocoles WAP et Web ne sont pas directement interopérables, un composant appelé passerelle WAP est nécessaire pour transformer les protocoles Web en WAP et vice versa.

B. Du sans fil à l'Internet

L'environnement internet WAP consiste à un client WAP, un réseau sans fil, une passerelle WAP, un réseau filaire IP, et un serveur de contenu Web.

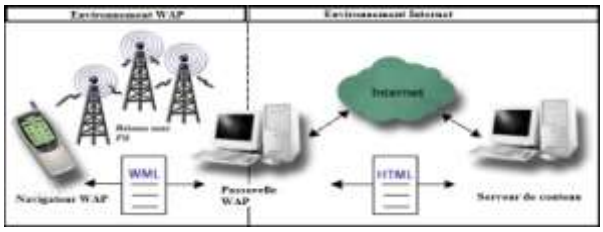

Figure 1. Les composants de l'environnement internet WAP (Source : Certicom)

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 [6]. 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 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 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 [7].

La figure 2 montre les trois parties impliquées dans une transaction m-commerce utilisant la technologie 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 connecté au réseau filaire (internet) [8].

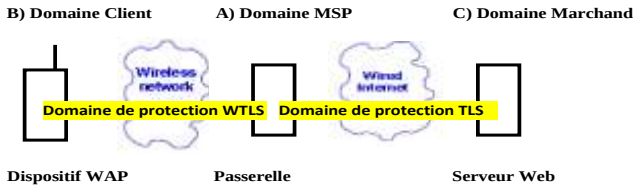

Figure 2. Les parties impliquées dans une transaction de type m-commerce utilisant le WAP.

C. *Le trou de sécurité de la passerelle WAP*

La passerelle WAP a pour mission de convertir des informations provenant de l'Internet au format WAP. 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 et vice versa, les données seront mises en texte clair, ce qui met en péril la session sécurisée [8].

Le WAP2 surmonte ce problème par des sessions sécurisées avec TLS/SSL de bout en bout. 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 et le chiffrement du texte [1,7].

IV. LES STANDARDS DE SECURITE DU WAP

Le WAP utilise plusieurs standards pour appliquer la sécurité aux niveaux application et transport dans l'environnement sans fil. Ces standards sont :

A. *WIM – Wireless Identity Module*

Une puce matérielle qui réside optionnellement dans le dispositif WAP. 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 [1, 5].

La figure 3 montre les opérations crytpo réalisés par le WIM : chiffrement et signature niveau application et authentification client niveau transport.

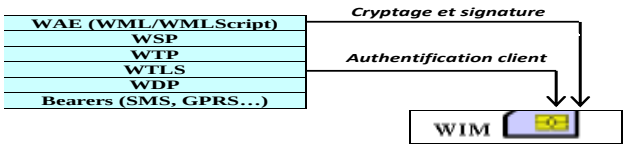

Figure 3. Le WAP et les niveaux de sécurité WIM

B. *WMLScrypt Crypto (WML Script Crypto API)*

Une API qui permet l'accès à des fonctions de sécurité dans une librairie WMLSCLib. Les fonctions de base dans 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, chiffrer et déchiffrer les données. WML Script peut utiliser un module WIM intégré pour fournir les fonctions de cryptographie [1, 5].

C. *WTLS/TLS*

Un protocole de sécurité niveau transport basé sur le protocole de sécurité internet connu sous le nom de SSL/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, la confidentialité par le chiffrement de données, et l'intégrité par l'emploi d'un MAC (Message Authentication Code).

La non-répudiation est fournie par un certificat WPKI. Le WAP définit un nouveau format de certificat optimisé en taille et fournit la même fonctionnalité que le certificat traditionnel X.509.

Le WAP2 avec Wireless Profile-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. Cependant, un problème majeur de performance se pose, à cause du temps pris par les calculs cryptographiques et la charge protocolaire du TLS.

D. *WPKI (Wireless Application PKI)*

Elle n'est pas une nouvelle PKI, mais une extension optimisée de la traditionnelle PKI pour l'environnement sans fil. La WPKI comme la PKI renforcent les règles de transactions m-commerce et gèrent la relation entre les parties communicantes, les clés et les certificats. Elle permet d'étendre le e-commerce aux environnements sans fil et mobiles [1,5].

V. LA WPKI (WIRELESS PUBLIC KEY INFRASTRUCTURE)

A. *L'architecture de la WPKI et son flux de données*

Le principe fondamental d'une PKI ne change pas dans les environnements sans fil. L'accès à un dispositif mobile 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. Elles 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 [1].

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 [1].

Un utilisateur final, non encore enregistré avec PKI, veut 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 cet 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. [1,5].

La WPKI nécessite les mêmes composants utilisés dans la PKI traditionnelle, mais l'application mobile et la RA sont optimisées pour les communications sans fil [1, 5].

Le diagramme de la figure 4 montre les principaux composants techniques et le flux opérationnel d'une WPKI.

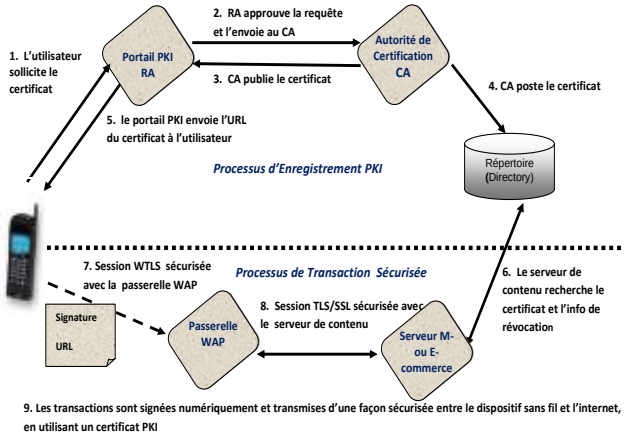

Figure 4. Les processus d'enregistrement PKI et de sécurité de la transaction avec WPKI

Le Portail PKI fonctionne logiquement comme une autorité d'enregistrement (RA) et est responsable de traduire les demandes faites par le client WAP à la RA et à la CA dans la PKI [1,5].

B. Les améliorations de la WPKI

La WPKI a optimisé en particulier les protocoles PKI, le format de certificat et les clés et les algorithmes cryptographiques [1, 5] :

1) *Les protocoles WPKI:* Les protocoles WPKI sont implémentés en utilisant le langage WML2 et l'API WMLSCrypt.
2) *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. Une autre réduction significative dans le certificat WPKI est l'utilisation de la cryptographie à courbe elliptique ECC.
3) *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 (ECC-163 bits vs. RSA-1024 bits). Ceci permet une optimisation dans le stockage de clé, la taille du certificat, l'utilisation de la mémoire et le calcul des signatures numériques.

VI. UN PROTOCLE DE SECURITE NIVEAU APPLICATION POUR UN SYSTEME M-COMMERCE UTILISANT LA TECHNOLOGIE WPKI

L'implémentation de la sécurité des communications sans fil nécessitent que les dispositifs et les réseaux mobiles supportent des technologies et des standards. Peu de dispositifs mobiles supportent le WAP1 et 2. Les opérateurs mobiles n'offrent pas tous des cartes SIM avec des modules WIM intégrés ou séparés. Par conséquent plusieurs modèles de sécurité niveau application basés WAP étaient proposés. Ces solutions emploient des signatures déléguées et un stockage de certificats dans un environnement sécurisé [9].

Cependant, dans toutes ces solutions proposées, la communication entre un dispositif mobile et un serveur de confiance n'est pas entièrement sécurisée.

Notre solution doit avoir le niveau de sécurité le plus élevé et qui correspond au WTLS classe 3 (authentification mutuelle avec des certificats WPKI, les clés publiques de la CA doivent être fournies au client et au serveur). Le chiffrement de données utilise un crypto-système asymétrique et seulement l'information sensible sera chiffrée. La sécurité est implémentée au niveau couche application, la fonction SignText de WMLScript Crypto (enrichie par le chiffrement) via l'utilisation du module WIM, permet respectivement d'authentifier le client auprès du serveur final et chiffrer ses données sensibles afin de s'assurer de leur confidentialité et de leur intégrité. Ce niveau élevé de sécurité peut être associé à des transactions importantes (e.g. macro paiement). Il suppose que le dispositif mobile intègre la technologie WAP et peut stocker les clés publiques/privées (un dispositif WAP avec WIM).

A. Description du Protocole de sécurité

Le Protocole proposé doit réaliser la sécurité de la transaction de bout en bout, il permet de réaliser l'authentification mutuelle entre le client et le serveur, chiffrer les données sensibles du client par la clé publique du serveur (pour qu'elles ne soient pas lisibles dans la passerelle), et signer numériquement la transaction pour assurer son intégrité. La signature numérique, sa vérification et le chiffrement de données utilisent des algorithmes basés sur une cryptographie ECC qui est mieux appropriée aux dispositifs mobiles et aux environnements sans fil. Pour 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.

La figure 5 montre l'architecture de ce Protocole de sécurité qui permet l'enregistrement WPKI d'un client mobile et la sécurisation de ses transactions. Le client est capable d'identifier l'identité de la passerelle. La passerelle peut aussi défier le client en lui envoyant des données à signer avec sa clé privée lorsque le client demande un certificat WPKI. De cette manière le client donne la preuve de sa possession de la clé privée associée à la clé publique de son certificat WPKI.

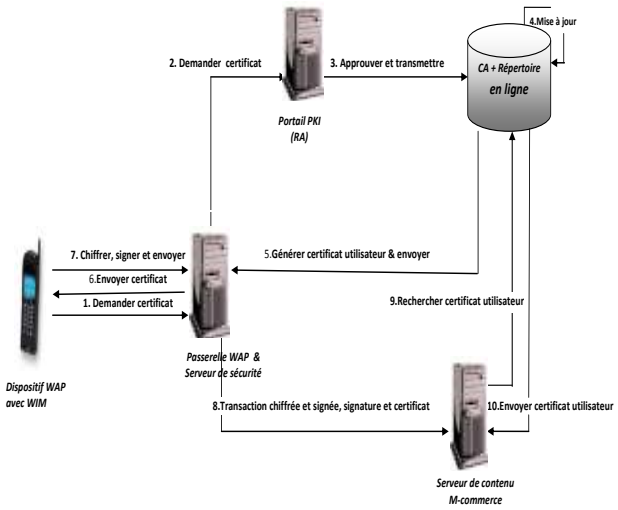

Figure 5. Protocole de sécurité niveau application basé WPKI pour les transactions du client mobile

La clé privée de l'utilisateur est stockée dans le module SIM ou WIM du téléphone mobile, alors le processus de signature vérifiant l'identité de l'utilisateur, peut être réalisé. Dans le cas ou le dispositif est volé ou perdu, et pour verrouiller la clé privée et sa fonction de signature associée, un code PIN est nécessaire. Personne ne peut accéder à la clé sans le code PIN. L'utilisateur doit entrer son code PIN pour permettre le chiffrement et la génération de la signature, ensuite la signature est envoyée au serveur comme preuve de non-repudiation.

L'implémentation de la sécurité au niveau application est réalisée comme suit :

1, 2 Le client demande un certificat d'un portail PKI via la passerelle.

3 Le portail PKI confirme l'identité de l'utilisateur et transmet la demande à la CA.

4, 5, 6 La CA génère le certificat utilisateur et transmet son URL au client via la passerelle. La CA peut envoyer le certificat complet au dispositif, il peut être stocké sur carte SIM/WIM. Si nécessaire, la CA met à jour sa base de données avec le certificat à clé publique de l'utilisateur.

7,8 Le client chiffre uniquement l'information sensible et signe la transaction avec la fonction *SignText* de WMLSCript. Il envoie la transaction, la signature et l'URL du certificat au serveur de contenu via la passerelle. Le serveur m-commerce peut avoir le certificat du client. Si le serveur n'a pas le certificat du client alors :

9 Le serveur utilise l'URL pour rechercher le certificat de l'utilisateur dans la base de données de la CA.

10 La CA transmet le certificat de l'utilisateur au serveur qui utilise alors la clé publique du client pour vérifier sa signature numérique. Le serveur utilise sa clé privée pour déchiffrer l'information sensible du client.

Ce Protocole de sécurité niveau application s'ajoute à la session de sécurité WTLS pour ne pas neutraliser les optimisations offertes par la passerelle WAP et qui comprennent la conversion et la compression de données afin de les adapter à la bande passante limitée des réseaux sans fil.

Il est basé sur le module WIM qui fournit un stockage sécurisé des clés, et des capacités de calcul cryptographique. Il permet l'exécution des protocoles de sécurité niveau WTLS et application (WALS-Wireless Application Layer Securite) au lieu qu'ils soient exécutés par le dispositif client (voir figure 6).

Autres protocoles avec des niveaux de sécurité moins élevés peuvent être utilisés pour des transactions moins importantes (micro paiement et mini paiement).

B. Protection des données sensibles

Ce Protocole de sécurité adopte deux schémas de chiffrement sur les données transmises et fournit une transmission plus sécurisée des données. La figure 7 montre la sécurité du processus de transmission de données sensibles de l'utilisateur mobile :

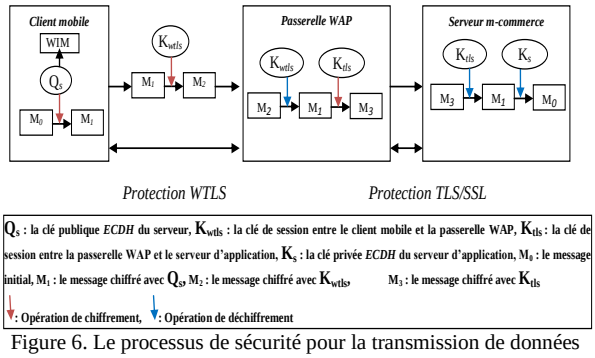

Figure 6. Le processus de sécurité pour la transmission de données sensibles

- Le client mobile chiffre le message M_0 qui contient les données sensibles avec la clé publique Q_s du serveur d'application (la clé publique du serveur peut être stockée dans le WIM) et obtient le message chiffré M_1. Le message M_1 est chiffré par la clé de session K_{wtls} pour avoir M_2 qui sera transmis à la passerelle WAP.
- La passerelle WAP déchiffre le message M_2 avec la clé K_{wtls} et obtient le message chiffré M_1. Elle chiffre M_1 avec la clé de session K_{tls}, et obtient M_3. Ensuite elle transmet M_3 au serveur d'application. Les données sensibles ne seront plus en texte clair dans la mémoire de la passerelle.
- Le serveur m-commerce déchiffre M_3 avec K_{tls} et obtient M_1, ensuite il déchiffre M_1 avec sa clé privée K_s et obtient le message original M_0.

C. Les certificats et les algorithmes crypto utilisés

Le client et le serveur doivent avoir chacun des certificats ECDH-ECDSA. Durant la phase de handshake WTLS, on vérifie les certificats, l'authentification mutuelle, et on génère le secret partagé ECDH qui sert pour produire la clé de session pour le chiffrement symétrique. La suite de chiffrement WTLS /TLS est basée sur un crypto système ECC pour l'établissement de la clé de session. On doit utiliser une suite de chiffrement implémentée qui donne le meilleur niveau de sécurité (e.g. TLS-ECDH-ECDSA-RC5-CBC-128-SHA1, TLS-ECDH-ECDSA-IDEA-CBC-128-SHA1 ou TLS-ECDH-ECDSA-3DES-CBC-SHA1). Le calcul de HMAC est basé sur la fonction de hachage SHA1.

Nous utilisons l'algorithme ECDH pour l'établissement et l'échange de la clé de chiffrement symétrique, et des

signatures ECDSA pour l'authentification mutuelle entre le client et le serveur. En d'autres termes, on utilise les services PKI relatifs au certificat X.509 basé ECC sur des dispositifs mobiles.

Une signature ECDSA n'augmente pas beaucoup la taille du message. Le message signé par ECDSA peut aussi être chiffré avec l'algorithme ECIES pour assurer la confidentialité du message.

Le client et le serveur exécutent chacun une opération ECDH pour établir le secret partagé après l'échange de leurs clés publiques ECDH. Le client mobile signe la transaction par sa clé ECDSA et chiffre les données sensibles par l'algorithme de cryptage ECIES en utilisant la clé publique ECDH (Qs) du serveur. Le serveur vérifie la signature du client par la clé publique ECDSA du client et déchiffre les données sensibles par sa clé privée ECDH (ks). Le client et le serveur ont des certificats clé publique ECDH basés sur les mêmes paramètres de courbe elliptique.

Tableau 1. Opérations crypto niveau application du client mobile

	Opérations crypto niveau application
Client	$ECDH_{op}$ + $ECDSA_{sign}$ + $ECIES_{encrypt}(Q_s)$
Serveur	$ECDH_{op}$ + $ECDSA_{verify}$ + $ECIES_{decrypt}$ (k_s)

D. Analyses pratiques

On considère deux approches pour comparer et mesurer la performance des algorithmes crypto utilisés : la sécurité et l'efficacité. La sécurité est la résistance aux attaques et elle est mesurée en nombre de bits composant la clé. Actuellement une paire de clé ECC 224 bits offre le même niveau de sécurité qu'une paire de clé RSA 2048 bits. L'efficacité a trois paramètres :

- La charge de calcul crypto : Certains paramètres dans le choix de courbes elliptiques EC peuvent être utilisés pour exécuter plus rapidement l'arithmétique modulaire utilisée dans l'opération ECC.
- La taille de la clé en nombre de bits pour l'espace du stockage : les clés ECC sont plus petites que celles de RSA ou DSA/DH.
- La bande passante : les crypto systèmes ECC offrent une économie considérable en bande passante. Ils sont mieux appropriés pour chiffrer et signer les messages de petite taille.

Nous avons réalisé des benchmarks d'opérations crypto dans la plateforme J2ME/MIDP et en utilisant l'API légère crypto de Bouncy Castle. Cette API a plusieurs caractéristiques : elle est open source, riche en algorithmes crypto et supporte la cryptographie ECC. Le tableau suivant compare les opérations crypto ECC avec celles de RSA:

Tableau 2. Comparaison des opérations crypto ECC PF vs RSA dans J2ME/MIDP

Opérations (ms)	**RSA-1024 bits**	**ECC 192-bits PF**	**RSA-2048 bits**	**ECC 239-bits PF**
Génération de paire de clés	3700,00	297,968	7030,00	468,34
Chiffrement	0,72	280,29	1,96	443,69
Déchiffrement	28,76	282,73	207,75	458,38
Signature numérique& vérification	30,19	690,53	212,48	1060,71

Nous pouvons remarquer que la génération de paire de clés RSA est une opération plus intensive que celle de ECC. Les autres opérations crypto ECC ne sont pas optimisées dans BC, mais en augmentant les tailles de clés (à partir de RSA-3072 bits), Il est évident que ECC offre un avantage de performance. D'après NIST, un crypto système ECC-256 bits est équivalent au niveau de sécurité à RSA-3072 bits:

Tableau 3. Comparaison de performance des opérations crypto ECC P-256 vs RSA-3072 dans J2SE

Opérations (ms)	**RSA-3072 bits**	**ECDSA-P256**
Génération de paire de clés	16499,902	33,352
Signature numérique & vérification	175,874	77,696

VII. CONCLUSION

Les standards du WAP ont étendu le contenu Internet et les transactions aux dispositifs sans fil. Les exigences de sécurité e-commerce sont les mêmes dans l'environnement filaire et l'environnement sans fil, 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 par l'utilisation d'une cryptographie plus efficace et appropriée aux environnements sans fil comme les algorithmes ECC.

Dans ce papier, nous avons proposé une solution de sécurité au niveau application basée WPKI pour sécuriser les transactions du client mobile et renforcer la session sécurisée WTLS. L'infrastructure de sécurité WPKI basée sur la cryptographie à clé publique ECC permet d'assurer la confidentialité, ainsi que l'intégrité des données de la transaction, et l'authentification des parties impliquées, au même temps que la non-répudiation.

RÉFÉRENCES

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

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

[3] Suranjan Choudhury, Kartik Bhatnagar, Wasim Haque, Public Key Infrastructure Implementation and Design, Published by M&T Books, 2002.

[4] V. Gayoso Martínez, L. Hernández Encinas, C. Sánchez Ávila, Elliptic Curve Cryptography. International Journal on Information Technologies & Security, № 4, 2009.

[5] Certicom Office Locations, Wireless Public-Key Infrastructure, Certicom Corporation 2001.

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

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

[8] Niels Christian Juul & Niels Jørgensen, WAP may Stumble over the Gateway (Security in WAP-based Mobile Commerce), Roskilde University, Denmark.

[9] Jasen Markovski & Marjan Gusev, Application level security of mobile communications, Ss. Cyril and Methodius University 2004.