UNIVERSITAT POLITÈCNICA DE BARCELONA

ESCOLA TÈCNICA SUPERIOR
D'ENGINYERIA DE TELECOMUNICACIÓN
DE BARCELONA

RESUMEN PROYECTO FIN DE CARRERA

Diseño e implementación de una pasarela de signatura digital con tecnología WAP

Autora: Helena Rifà Pous
Tutor: Francisco Jordán Fernández
Departamento: Arquitectura de Computadores
Empresa: Safelayer Secure Communications, S.A.
Fecha de lectura: 16/02/2001
Calificación: 10 Matrícula de Honor

SAFELAYER
SECURE
COMMUNICATIONS S.A.

ÍNDICE

1. INTRODUCCIÓN

El sector de las tecnologías de la información es uno de los que más cambios ha sufrido en los últimos años y uno de los principales motores de la economía actual. Si la década de los noventa vino marcada por la revolución de Internet, las comunicaciones a través de redes inalámbricas supondrán un cambio de paradigma en este principio de milenio.

La necesidad de estar en línea en cualquier momento, lugar y situación ha dado a WAP la oportunidad de emerger rápidamente como estándar global de comunicaciones móviles a Internet. Los terminales sin hilos son dispositivos mucho más pequeños, con menos memoria y menos capacidad de procesador que los típicos ordenadores de sobremesa. Además, las redes de comunicaciones móviles tienen poco ancho de banda y una disponibilidad ligeramente irregular. Es por eso que se ha creado este nuevo estándar paralelo al de Internet; pero aunque WAP ha heredado muchas de las características de la WEB, los dos no son compatibles.

Se espera que en los próximos años las aplicaciones de comercio a través de móvil crezcan de manera espectacular. El continuo avance de las tecnologías de seguridad junto al que se está produciendo en las redes y protocolos de telefonía móvil facilitarán la prestación de servicios de *m-commerce*.

Este proyecto se centra en los aspectos de seguridad del WAP y su implicación en el mercado de los móviles. Los servicios de comercio electrónico a través de móviles que existen actualmente no tienen en cuenta todos los aspectos de seguridad necesarios para hacer transacciones sin riesgos. Esto se debe a varios motivos:

- Si bien hay especificaciones que ya han definido protocolos para hacer transacciones seguras, la tecnología aún no está disponible o la implantación de esta tecnología a nivel masivo supone cambiar los parques de tarjetas SIM y terminales casi al completo.

- Aun estando resueltos los aspectos tecnológicos anteriores apenas existen experiencias reales en las que se hayan empleado estas tecnologías.

El comercio electrónico ya está empezando a incidir en la forma de adquirir bienes y servicios de muchas personas, pero aún no ha habido el boom que muchos analistas predecían, y eso es debido, en gran parte, a la falta de confianza de los usuarios. Las aplicaciones que requieren la gestión de datos confidenciales tienen un compromiso entre la seguridad de la operación y la facilidad de utilización de la aplicación.

WAP pretende ser el equivalente a TCP/IP en el entorno móvil, y será el único medio de acceso a Internet para una gran población sin los recursos necesarios para mantener un ordenador con la única funcionalidad de conectarse a la red. La utilización de un teléfono móvil no es la forma más cómoda de acceder a Internet, y se prevé que la mayor parte de accesos que se hagan a través de este sistema sean para temas puntuales y de importancia relevante, como aplicaciones de banca electrónica, borsa, transacciones o simplemente correos electrónicos. Es importante desarrollar aplicaciones claras, sencillas, robustas y sobretodo seguras, pues la mayor parte de operaciones usarán datos privados y requerirán un canal de transporte fiable.

La tecnología PKI (Public Key Infrastructure) – para móviles WPKI - la tecnología WAP, concretamente el protocolo WTLS, y las nuevas generaciones de tarjetas criptográficas para terminales celulares (SWIM para redes GSM y USIM para UMTS) serán capaces de proporcionar mecanismos de seguridad más avanzados y orientados tanto a las necesidades propias de la

telefonía móvil como a servicios de valor añadido, convirtiendo al terminal en un dispositivo de seguridad portátil.

El proyecto tiene como objetivo diseñar e implementar una aplicación que permita enviar mensajes de correo signados a través de teléfonos móviles. La estructura del prototipo tendrá que permitir que estos correos electrónicos se puedan enviar con los terminales actuales (sin muchas o ninguna infraestructura criptográfica) y también con terminales futuros que tendrán implementadas más funcionalidades. Se pretende que la aplicación incluya los mecanismos de seguridad necesarios para garantizar la autenticidad y la integridad de los datos. Por ello se tendrá que montar un entorno PKI (y WPKI) que le de soporte. Deberemos tener unas autoridades de certificación que emitan certificados con la estructura descrita en WAP y permitan gestionar la dualidad de estructuras móvil/red fija.

Los objetivos que se persiguen son:

- Analizar la compatibilidad entre los estándares de WPKI y los de PKI.
- Generar certificados WTLS para móviles e instalarlos en los terminales.
- Adquirir experiencia en aspectos de seguridad relacionados con pago electrónico, especialmente en la Firma electrónica como mecanismo de no repudio de transacciones.
- Diseñar e implementar una pasarela que permita enviar mensajes de correo signados (SMIME) a través de un teléfono móvil.
- Implementar una aplicación que emule la tarjeta criptográfica WIM del protocolo WAP en sus funciones de firma digital.
- Crear una maqueta que sirva de demostrador de la funcionalidad del empleo de mecanismos de seguridad avanzados en los móviles.
- Crear la base sobre la cual realizar futuros y más complejos pilotos basados de WPKI.

El proyecto presentado se realizó en la empresa Safelayer Secure Communications, S.A. compañía dedicada al desarrollo de productos en las tecnologías de PKI y SET (estándar de comercio electrónico).

La presente memoria es un resumen del trabajo realizado en el proyecto. En primer lugar se hace una introducción a la tecnología WAP y se explican las motivaciones que han llevado a crear un estándar para dispositivos móviles. Se verá la arquitectura de WAP y las características de seguridad que se han definido en la especificación. A continuación se explica la aplicación realizada que permite enviar mensajes firmados desde teléfonos móviles WAP sin prestaciones criptográficas o que dispongan de tarjetas WIM. Finalmente se hace una valoración del protocolo y se extraen conclusiones del trabajo realizado.

2. TECNOLOGÍA WAP

2.1 Inicios y motivaciones de WAP

WAP, o Protocolo de Aplicaciones Inalámbricas, es un conjunto de nuevos estándares diseñados para extender los servicios de Internet al entorno de la telefonía móvil. El desarrollo del protocolo está coordinado por el Wap Forum, una organización formada por las más importantes industrias del sector, y que tiene la misión de llevar los mejores principios del desarrollo de aplicaciones Internet a la comunidad inalámbrica.

A partir de 1995 empezaron a nacer protocolos para dar servicios de valor añadido a las redes inalámbricas. Debido al peligro que suponía que el mercado se fragmentara y terminara disolviéndose, el diciembre de 1997 cuatro empresas (Ericsson, Motorola, Nokia y Unwired Planet)

unieron esfuerzos y crearon el Wap Forum con el objetivo de impulsar un único estándar de servicios avanzados en el dominio de redes sin hilos. Después del lanzamiento de las especificaciones WAP 1.0 en abril de 1998, se abrió a todo el mundo la posibilidad de ser miembro del Wap Forum.

WAP está en el punto de convergencia de dos tecnologías emergentes, la información a través de móvil e Internet. Estos dos mercados han crecido mucho en los últimos años llegando cada vez a nuevos consumidores. La mayor parte de la tecnología desarrollada por Internet ha estado diseñada para grandes ordenadores de sobremesa con medio o gran ancho de banda sobre una red de datos fiable. El entorno de los dispositivos móviles de mano presenta unas características más limitadas que se tienen que tener en consideración a la hora de intentar unir las dos tecnologías.

Por lo que hace referencia a los terminales móviles, las principales limitaciones son las siguientes:

- CPUs de poca potencia
- Poco memoria ROM y RAM
- Consumo de potencia restringido
- Pantallas pequeñas
- Diferentes tipos de dispositivos de entrada (un teclado de teléfono, entrada de voz,...)

Las redes de datos móviles presentan, en comparación a las redes cableadas, las siguientes características:

- Menos ancho de banda
- Más retardos
- Menos estabilidad en las conexiones
- Disponibilidad poco predecible

Además hay un compromiso entre las limitaciones del terminal y las de la red ya que al aumentar el ancho de banda, también aumenta el consumo de los terminales, disminuyendo de esta forma el tiempo de vida de la batería.

La posibilidad de tener cualquier información disponible en un terminal inalámbrico en cualquier momento, abre un nuevo mercado de acceso a la información. Este mercado es muy diferente del de los ordenadores de sobremesa e incluso de los portátiles, ya que el usuario de un teléfono móvil tiene necesidades diferentes, y espera ver la información de manera diferente a un navegador WEB.

- Facilidad de uso: Los teléfonos tienen un mercado mucho más amplio que los ordenadores, y por lo tanto serán utilizados por personas sin experiencia informática.
- Precio: La demanda es muy elástica, es importante que los terminales mantengan el coste bajo.

- Tascas esenciales: Los usuarios querrán realizar tareas muy concretas y de manera rápida.

2.2 Arquitectura WAP

Wap Forum, al cabo de menos de un año de su fundación, sacó la especificación WAP 1.0. En el momento de realizar el proyecto la versión disponible en los móviles era la WAP 1.1 y se estaba trabajando en la WAP 2.0. En este trabajo nos centraremos en la versión WAP 1.2, que era la última que había estado aprobada entonces, pero también se hará referencia a las mejoras que incorpora con respecto a la que los móviles tenían implantada y a las nuevas funcionalidades se preveían para el futuro.

Las especificaciones WAP surgen a partir de la adopción de la tecnología Internet a las restricciones del sistema inalámbrico. Las características clave que presenta WAP son las siguientes:

- Un modelo de programación similar al de Internet

Como los navegadores Web, los dispositivos WAP se basan en una serie de transacciones pregunta/respuesta con los servidores de contenidos.

- WML *(Wireless Markup Language)*

WML es un lenguaje de marcas basado en XML y diseñado para crear aplicaciones WAP independientes del dispositivo utilizado. De la misma forma que el HTML en el WWW, el WML se centra en presentar contenidos formateados y opciones de ejecución limitadas a los usuarios.

- WMLScript

El WMLscript es un lenguaje de scripting basado en el ECMAScript y que tiene por objetivo extender las funcionalidades del WML. A diferencia del WML, que se basa en lo que el usuario ve, el WMLScript tiene muy pocas capacidades de interfaz con el usuario. En lugar de esto, está diseñado para agregar procedimientos lógicos y capacidades computacionales robustas a WML.

- Especificación de un micronavegador

El Wap Forum define las funcionalidades y el interfaz de usuario mínimo que el dispositivo WAP tiene que tener. Se define como deben ser interpretados y presentados al usuario los lenguajes WML y el WMLScript.

- Marco para WTA *(Wireless Telephony Application)*

El marco WTA proporciona finalidades que las operadoras telefónicas pueden utilizar para integrar funciones de telefonía en el navegador. Por ejemplo, se pueden crear aplicaciones en WML que permitan controlar las llamadas entrantes, recuperar mensajes de voz, redireccionar llamadas o cambiar entradas en la libreta de direcciones.

- Pila de protocolos optimizada

Pila de protocolos diseñada para minimizar los requerimientos de ancho de banda, trabajar con gran variedad de transportes móviles y proporcionar conexiones seguras. Se intenta que el estándar desarrollado se pueda escalar a una gran variedad de terminales móviles y redes.

El modelo de programación WAP es muy similar al modelo WEB con dos diferencias fundamentales:

- Presencia de una pasarela WAP entre el agente de usuario y el navegador de contenidos. La principal función de este componente es la de traducir los protocolos WAP del dispositivo móvil a HTTP con el fin de comunicarse con el servidor de contenidos, y vice-versa. También puede tener que compilar las aplicaciones WML y WMLScript creadas dinámicamente por el servidor de contenidos.

- La comunicación entre el agente de usuario y las pasarela WAP se hace con los protocolos WAP. El más importante de estos es el WSP (Wireless Session Protocol), que en esencia es una forma compacta y binaria de http 1.1.

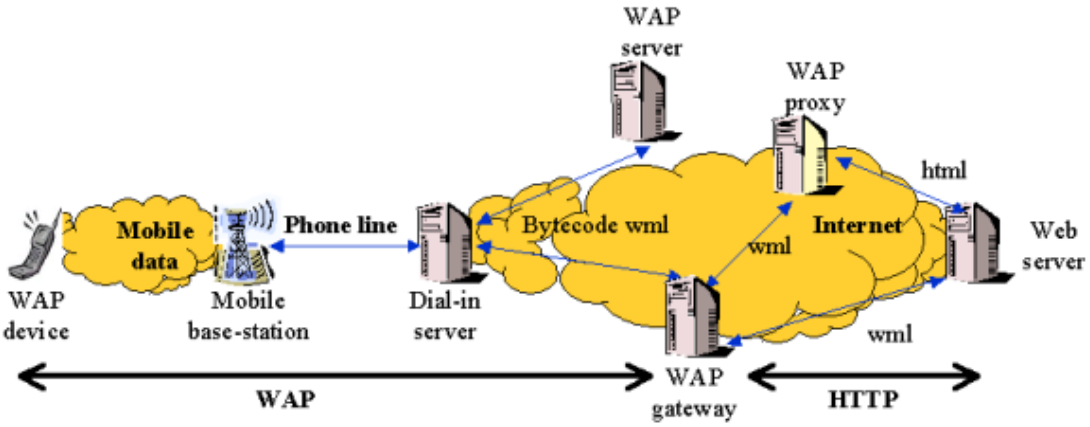

Figura 1: Esquema de una conexión WAP

En la figura *1* se muestra el esquema general de una conexión a Internet desde un teléfono WAP. Los pasos realizados son los siguientes:

1. El teléfono realiza una conexión PPP (dial-up TCP/IP) con el servidor RAS *(Remote Access Server)*.

2. Sobre la conexión RAS el teléfono enviará y recibirá paquetes sobre UDP en la conexión con la pasarela WAP.

3. La pasarela WAP traduce las peticiones de los móviles a HTTP, y los resultados son compilados y transmitidos a su vez al teléfono.

El móvil tiene 3 posibilidades de interconexión: a una pasarela WAP, a un servidor WAP (que hace las funciones de la pasarela y del servidor de contenidos a la vez), o a un servidor WTA (permite el acceso WAP a las facilidades proporcionadas por la infraestructura de telecomunicaciones del proveedor de conexiones de la red). El hecho de que exista una pasarela WAP es debido a razones de compatibilidad. Con esta configuración los desarrolladores de aplicaciones no tienen que aprender una nueva arquitectura tecnológica y pueden reaprovechar todos los conocimientos de programación WEB. Además, los proveedores de servicios no necesitan invertir en nueva infraestructura ya que los servicios de la pasarela WAP los ofrece el operador de comunicaciones. El problema es que con esta arquitectura el servidor de contenidos tiene muy poco control de lo que ocurre en la pasarela y a veces necesita poder gestionar las características de la transmisión con el cliente final. Es por este motivo que existen los servidores WAP, uno servidores que son capaces de entregar páginas compiladas WML y WMLScript a través del protocolo de sesión de WAP WSP.

2.2.1 COMPONENTES DE LA ARQUITECTURA WAP

WAP está diseñado jerárquicamente para ser extensible, flexible y escalable. Por eso se define una estructura en capas, en la cual cada capa es accesible por la capa superior así como por otros servicios y aplicaciones a través de un conjunto de interfaces muy bien definidos y especificados. En la figura 2 podemos ver la pila de protocolos WAP y como se relacionan con los protocolos Internet.

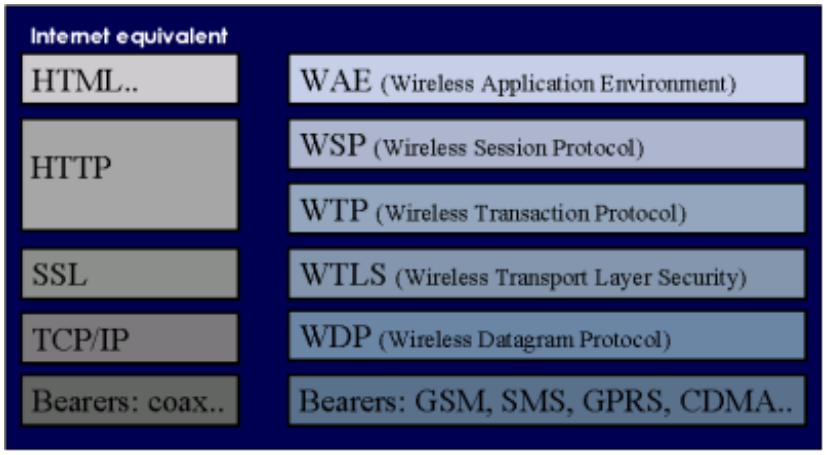

Figura 2: Arquitectura WAP

A continuación exponemos de forma breve cuales son las principales características de estas capas:

- Nivel de aplicación: WAE

  El entorno inalámbrico de aplicación define el interfaz del usuario con el teléfono. Es un entorno de aplicación de propósito general basado en la combinación de la WWW y de las

tecnologías de comunicaciones móviles. Este entorno incluye un micronavegador que tiene herramientas para el desarrollo de servicios en WML, WMLScript y WTA.

- Nivel de sesión: WSP

  El protocolo inalámbrico de sesión proporciona a la capa de aplicación WAP un interfaz con dos servicios de sesión: un servicio orientado a conexión que funciona por encima de la cada de transacción, y un servicio no orientado a conexión que funciona sobre la capa de transporte.

- Nivel de transacción: WTP

  El protocolo inalámbrico de transacción funciona por encima de un servicio de datagramas. Ofrece 3 clases de servicio: peticiones no fiables, peticiones fiables de un solo sentido y transacciones fiables en los dos sentidos (petición-respuesta). Proporciona funcionalidades de fiabilidad opcional usuario-usuario, reconocimiento de datos fuera de banda, transacciones asíncronas y concatenación de PDUs (Protocol Data Unit), y reconocimientos retardados por tal de reducir el número de mensajes enviados.

- Nivel de seguridad: WTLS

  La capa inalámbrica de seguridad de transporte está basada en el estándar TLS. Se ha diseñado por tal de ser utilizada con los protocolos de transporte WAP, y ha estado optimizada para funcionar en canales de comunicaciones de poco ancho de banda. Las funcionalidades que proporciona WTLS son integridad de los datos, privacidad y autenticación.

- Nivel de transporte: WDP

  El protocolo inalámbrico de datagramas proporciona un servicio fiable a los protocolos de las capas superiores de WAP y permite la comunicación de forma transparente sobre los protocolos portadores válidos. Como este protocolo proporciona un interfaz común a los protocolos de las capas superiores, las capas de seguridad, sesión y aplicación pueden trabajar independientemente de la red inalámbrica que diese suporte al sistema.

- Portadoras

  Los protocolos WAP están diseñados para operar sobre diferentes servicios portadores, incluyendo los mensajes cortos SMS y las redes de comunicación de circuitos o paquetes. La especificación de WDP lista las portadoras suportadas y las técnicas utilizadas para permitir que los portadores WAP operen sobre cada portadora. Esta lista de portadoras irá cambiando con el tiempo a medida que nuevas tecnologías aparezcan en el mercado de los móviles.

2.2.2 SEGURIDAD EN WAP

Posibilitar las transacciones seguras en WAP ha estado siempre uno de los objetivos del WAP Forum ya que las aplicaciones de comercio electrónico son uno de los principales reclamos para comprar terminales que dispongan de esta nueva tecnología.

En las conexiones a Internet desde dispositivos móviles, los datos son transferidos a través de diferentes canales: por aire, por la línea telefónica y sobre redes IP. La seguridad que ofrecen los protocolos de telefonía móvil como el GSM no es suficiente ya que están limitados a la etapa aérea. Además, la fortaleza de los algoritmos criptográficos A5/1 y A5/2 utilizados en GSM es altamente cuestionada ya que se ha comprobado que pueden ser rotos en pocos segundos por simples PCs. Es por este motivo que WAP incorpora sus propios sistemas para transferir información de forma segura.

La seguridad en WAP es abordada en las siguientes especificaciones:

- Protocolo inalámbrico de seguridad a nivel de transporte: WTLS
- Librería criptográfica del lenguaje WMLS: WMLScript Crypto Library
- Módulo de identidad inalámbrico: WIM

El modelo general de PKI para entornos WAP (WPKI) define las funciones necesarias para gestionar los aspectos de seguridad de WAP 1.2.

WTLS

WTLS es un protocolo de transporte seguro basado en el protocolo de seguridad en Internet TLS v1.0. No se utiliza el TLS debido a los requisitos especiales de las redes sin hilos:

- Tienen que estar suportados tanto los niveles de transporte orientados a conexión como en modo datagrama.
- El protocolo tiene que ser capaz de funcionar con retardos importantes.
- El ancho de banda de algunas portadoras puede ser muy bajo.
- La potencia de proceso de los terminales móviles es bastante limitada.
- La capacidad de memoria de los dispositivos inalámbricos es pequeña.

El WTLS ha estado optimizado para redes portadoras de poco ancho de banda y retardos relativamente grandes, por eso se han incorporado nuevas funcionalidades a las proporcionadas por TLS, como soporte a datagrama, un modo optimizado de intercambio de claves, y refresco dinámico de la clave de sesión para dificultar más los ataques en un medio de transmisión tan vulnerable a espías.

Criptográficamente las innovaciones de WTLS son mínimas. La más significativa es que admite la utilización de algoritmos criptográficos basados en curvas elípticas (EDC: Diffie-Hellman basado en curvas elípticas) para el intercambio de claves que ofrecen algunas ventajas en cuanto a memoria y prestaciones. Los otros algoritmos que soporta son los ya conocidos en TLS: DH (Diffie-Hellman) y RSA para el intercambio de claves simétricas, RC5, DES, 3DES y IDEA para el cifrado simétrico, y MD5 y SHA para la generación de los MACs. Además, la especificación permite el uso de certificados X.509, WTLS (Similares a los X.509v1. Han sido optimizados para reducir el tamaño. Son obligatorios si el intercambio de claves no es anónimo) y X9.68 (certificados basados en curvas elípticas).

WTLS ofrece seguridad extremo-extremo entre los puntos finales del protocolo WAP. Realmente los extremos del protocolo son el terminal móvil y la pasarela WAP. Cuando la pasarela hace peticiones al servidor origen utiliza SSL bajo HTTP para obtener confidencialidad. Como los protocolos WTLS y SSL no son compatibles, los datos tienen que ser descifrados y vueltos a cifrar en la pasarela. El hecho de que los datos residan en claro unos instantes en la pasarela es uno de los puntos más criticados del protocolo WAP.

WMLScript Crypto Library

Muchos tipos de aplicaciones como el comercio electrónico requieren la capacidad de poder proporcionar pruebas persistentes de la autorización que alguien ha dado para hacer una determinada transacción. Aunque WTLS proporciona autenticación transitoria del cliente para la duración de la conexión WTLS, esta validación no es válida como autenticación persistente de las transacciones que puedan ocurrir durante la conexión. Una forma de dar este tipo de autenticación es asociar una signatura digital a los datos generados como resultado de la transacción, que por ejemplo puede ser una orden de compra o algún otro documento financiero.

Por tal de suportar este requisito, el navegador WAP incluye una función en la librería criptográfica de WMLScript, la Crypto.signText(), que signa un campo de texto de un formulario WML. Una llamada a esta función permite signar cualquier cadena de la página WML, que se mostrará por pantalla para pedir al usuario su confirmación. Después que los datos hayan sido firmados y tanto la signatura como los datos hayan sido enviados a través de la red, el servidor puede extraer la firma digital, validarla y guardarla para propósitos contables.

WIM

Como hemos visto en los puntos anteriores, la funcionalidad de seguridad en WAP incluye el protocolo WTLS a nivel de transporte, y el WMLScript a nivel de aplicación. Para una seguridad óptima, algunas de las partes de las funciones de seguridad necesitan ser computadas en un dispositivo hardware protegido, de manera que un atacante no pueda extraer datos susceptibles. Estas funciones son las que incluyen datos sensibles, concretamente las claves privadas permanentes utilizadas en el establecimiento de conexión WTLS con autenticación de cliente y las claves que se utilizan en la generación de signaturas electrónicas en el nivel de aplicación. Por lo tanto, el módulo de Identidad WAP sirve para realizar la funciones de seguridad en WTLS y WMLScript, y especialmente, para guardar y procesar la información necesaria para identificar y autenticar al usuario.

3. APLICACIÓN

La aplicación desarrollado consiste en el conjunto wMail Secure Gateway de la figura 3. Básicamente se trata de dos módulos cliente/servidor (WAE Web & lDAP Server y WMLScript SMIME gateway) que permiten a los usuarios de teléfonos móviles enviar mensajes de correo signados con el estándar SMIME.

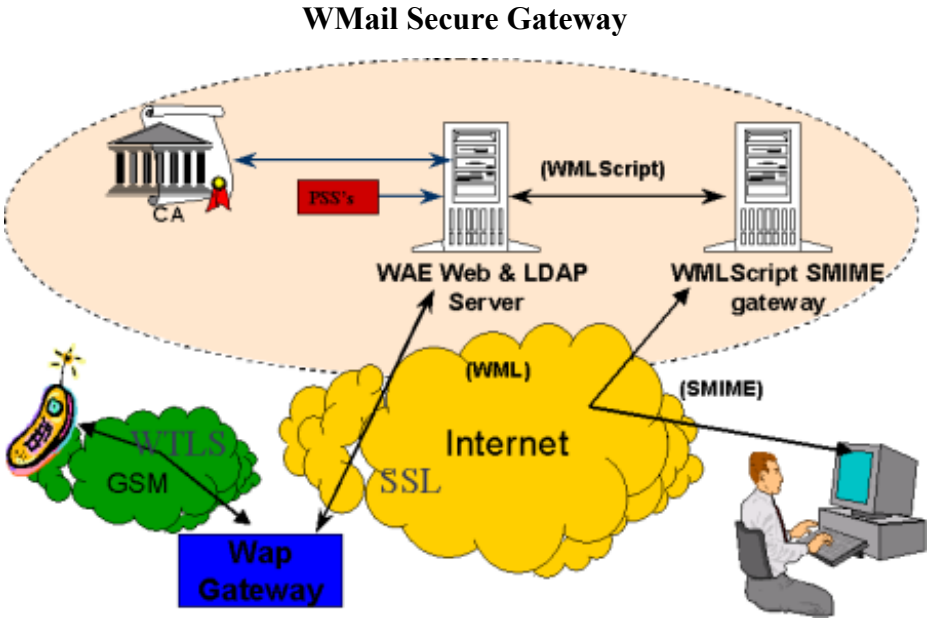

Figura 3: wMail

El módulo WAE Web & LDAP lleva a cabo las funciones criptográficas del cliente a través de un interfaz WML. El micronavegador se conecta con el servidor Web WAE con una comunicación segura y se autentica en este servidor con nombre y contraseña. La conexión es segura ya que la URL del módulo WAE requiere SSL. La parte inalámbrica de la comunicación (entre la pasarela de la operadora de telefonía móvil y el terminal del cliente) puede ser securizada con WTLS, y es responsabilidad del cliente asegurar que la conexión se establece con este protocolo.

En el entorno seguro de WAE, los usuarios puede gestionar sus claves privada y sus certificados, que se almacenan en un PSS (un objeto seguro protegido contra el acceso ilícito o las modificaciones) y son publicados en un LDAP. El usuario puede crear certificador X.509 y WTLS, ya que el estándar WPKI permite los dos tipos de certificados.

El interfaz WML del módulo WAE también permite signar digitalmente mensajes con el estándar definido en la librería criptográfica WMLScript Crypto.

El servidor WAE tiene un interfaz HTML que permite a los usuarios gestionar sus cuentas de forma más sencilla. A través de la web se pueden crear certificados, organizar la libreta de direcciones, cambiar la contraseña del usuario y analizar el formato de signatura de WMLScript a partir de las funciones de parseo.

El módulo WMLScript-SMIME gateway traduce los mensajes firmados de formato WMLScript a SMIME sin poner en peligro la seguridad extremo a extremo. WMLScript-SMIME gateway es una aplicación con un interfaz WML y por tanto, permite enviar mensajes provinentes de cualquier cliente que sepa signar con el estándar WMLScript.

En este sistema se han integrado las siguientes tecnologías: HTML/Web, WML/Wap, LDAP, certificados X.509 y certificados WTLS, PKCS#, WAP WMLScript Signature y S/MIME. Todas las aplicaciones se han desarrollado con lenguajes de programación WEB y WAP, y con CGIs en C++ en la parte servidor. Se ha utilizado la API J++ASN de Safelayer Secure Communications que proporciona funcionalidades criptográficas y herramientas para el desarrollo de protocolos con especificaciones ASN.1. Se ha construido una librería de gestión de mensajes WAP que permite crear y verificar mensajes firmados, hacer traducciones de signaturas WAP a formatos PKCS#7 y SMIME, y gestionar búsquedas de certificados equivalentes WTLS/X.509.

Para más información y demostración ver las siguientes direcciones:

- WEB: http://node.safelayer.com/wap/wap_index_es.html
- WAP: http://node.safelayer.com/

3.1. Certificados WTLS

El único formato de certificados que los móviles tienen que aceptar obligatoriamente son los WTLS. Uno de los productos de Safelayer es una Autoridad de Certificación. Se han extendido las funcionalidades de esta autoridad para que pueda emitir también certificados WAP.

Se ha creado una aplicación de demostración en Internet que permite obtener certificados WTLS de usuario a partir de una petición de certificación con formato PKCS#10.

```
WTLSCertificate struct {
  to_be_signed_certificate struct {
    certificate_version uint8;
    signature_algorithm SignatureAlgorithm;
    issuer Identifier;
    valid_not_before uint32;
    valid_not_after uint32;
    subject Identifier;
    public_key_type PublicKeyType;
    parameter_specifier ParameterSpecifier;
    public_key PublicKey;
    } signature Signature;
}
```

También se han generado certificados WTLS de servidor que pueden descargarse en los móviles y permiten realizar transacciones sobre una canal seguro con autenticación de pasarela (el cliente puede confiar en la pasarela ya que reconoce su certificado como válido).

3.2. Interfaz WAP de wMail Secure Gateway

WMail Secure Gateway está formado por los módulos WAE Web & LDAP y WMLScript SMIME Gateway. La parte WAE Web engloba las funciones de interfaz con el usuario, que pueden ser mediante WEB o WAP. La pasarela WMLScript-SMIME hace una traducción del formato signado propio de WAP y compatible con PKCS#7, al formato SMIME.

El objetivo de la pasarela wMail es que pueda traducir mensajes signados creados por móviles, a el estándar SMIME de Internet. El primer problema es que los teléfonos actuales no soportan WPKI y no pueden almacenar claves públicas ni privadas. Además, no disponemos de herramientas para programar las tarjetas SIM y dotar de capacidades criptográficas al teléfono. Para suplir estas deficiencias se crea el módulo WAE que proporcionará esta parte 'inteligente' al móvil. Las funcionalidades del módulo WAE serán:

- Comunicación segura con el usuario para proporcionarle funcionalidades de gestión de los elementos criptográficos personales.

- Almacén seguro de certificados y llaves privadas

- Funciones de autoridad de certificación para emitir certificados personales a los usuarios de móviles.

- Funciones de publicación de certificados en WEB y en LDAP.

- Funciones para signar mensajes digitalmente con el formato signedContent de la librería WMLScript.Crypto.

- Interfaz WML para proporcionar al usuario la funcionalidad de signar mensajes de forma análoga a como lo haría la función Crypto.signText().

La salida del módulo WAE será un objeto signado con el formato signedContent de WAP, compatible con el estándar PKCS#7 pero no con SMIME. Los clientes de correo electrónico no entienden este formato y por lo tanto no tiene ningún sentido enviarles un mensaje así. Lo que se hará es redirigir la salida del módulo WAE Web & LDAP a la pasarela WMLScript-SMIME para que haga la traducción entre estos dos formatos. El mensaje en claro no estará incluido en el PKCS#7 que contiene la signatura, sino que se adjuntará de forma independiente de manera que los clientes que no soportan funcionalidades criptográficas puedan leer el correo.

Las características principales de la pasarela son:

- Creación de un mensaje SMIME a partir de los datos de un formulario WML

- Conexión a centros de publicación de certificados

- Confirmación del resultado del proceso a la aplicación que ha mandado los datos

- Enviar el mensaje SMIME al destinatario del correo

Los pasos seguidos para que un usuario pueda enviar un mensaje SMIME desde su móvil son los siguientes: (figura 4)

1. El usuario pide un certificado a través de su teléfono móvil conectándose al servidor WAE.

2. El módulo WAE confirma la identificación del usuario y pasa la petición a la Autoridad de Certificación (CA).

3. La CA genera dos certificados de usuario (uno WTLS y otro X.509) con las mismas claves criptográficas. Estas claves se envían al PSS (repositorio seguro) que contiene el servidor WAE junto con los certificados creados.

4. La CA pone los certificados de usuario creados en una base de datos pública que permite conexiones URL, y en un directorio LDAP.

5. El usuario entra en la página WML del servidor WAE y escribe el texto que quiere firmar.

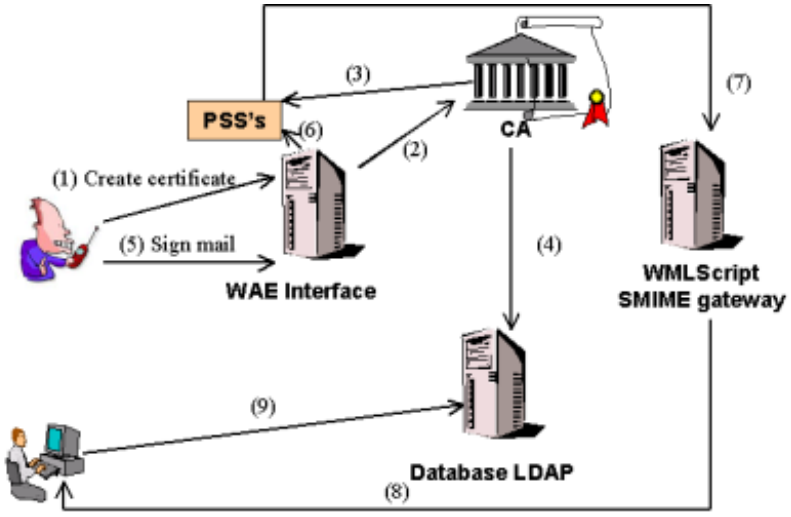

Figura 4: Esquema de una conexión WAP

6. El modulo WAE confirma la identidad del usuario y envía el nombre de usuario y la contraseña al PSS con tal de obtener la clave privada.

7. El PSS verifica la contraseña del usuario y devuelve la clave y el certificado asociado a ésta.

8. El módulo WAE signa el mensaje y envía el contenido signedContent resultante a la pasarela WMLScript-SMIME.

9. La pasarela WMLScript-SMIME traduce la estructura signedContent de WAP a un correo SMIME, y lo enviar a la cuenta POP3 del destinatario.

10. El cliente de correo recibe el mensaje y verifica la signatura bajándose el certificado del cliente (si es necesario) y el certificado raíz de la base de datos.

A nivel de usuario, las opciones para llevar a término el proceso de signatura se pueden resumir en la figura *5*.

Figura 5: Demostración del interfaz de usuario WAP

1. El usuario entra en el portal de firma de mensajes

2. La zona privada de cada usuario está restringida mediante nombre de usuario y contraseña

3. Las funcionalidades de la parte confidencial de la aplicación están relacionadas con la gestión de los certificados. El cliente escoge la opción de enviar un mensaje signado

4. Se introduce la información del correo electrónico que se quiere enviar. Se dispone de una libreta de direcciones (configurable por WEB) que facilita la entrada de datos.

5. Una vez escrito el mensaje, la aplicación pide que el usuario escoja el certificado con el que quiere firmar el texto. Se soportan certificados WTLS y X.509.

6. Se envía el mensaje al módulo WAE Web que será el encargado de realizar la firma y enviar los datos a la pasarela WAP/SMIME para que genere un mail signado.

Si en el cliente de correo instalamos y confiamos en el certificado raíz de la Autoridad de Certificación que emitió los certificados de usuario usados, se podrá validar la firma (ver figura 6).

Figura 6: Mensaje recibido

3.3 Interfaz WEB de wMail Secure Gateway

Gestionar una cuenta de correo electrónico desde el móvil puede ser largo y pesado. Una aplicación WAP sólo es útil si permite hacer tascas concretas de forma sencilla y rápida ya que las velocidades de transmisión son aún muy lentas, los precios de conexión elevados, y el interfaz de entrada de datos complicado. Es por estos motivos que se ha creado un interfaz WEB en el módulo WAE que permite a los usuarios gestionar su zona personal de igual forma que se podría hacer desde un teléfono, e incluso añadiendo alguna funcionalidad más como la de crear una libreta de direcciones.

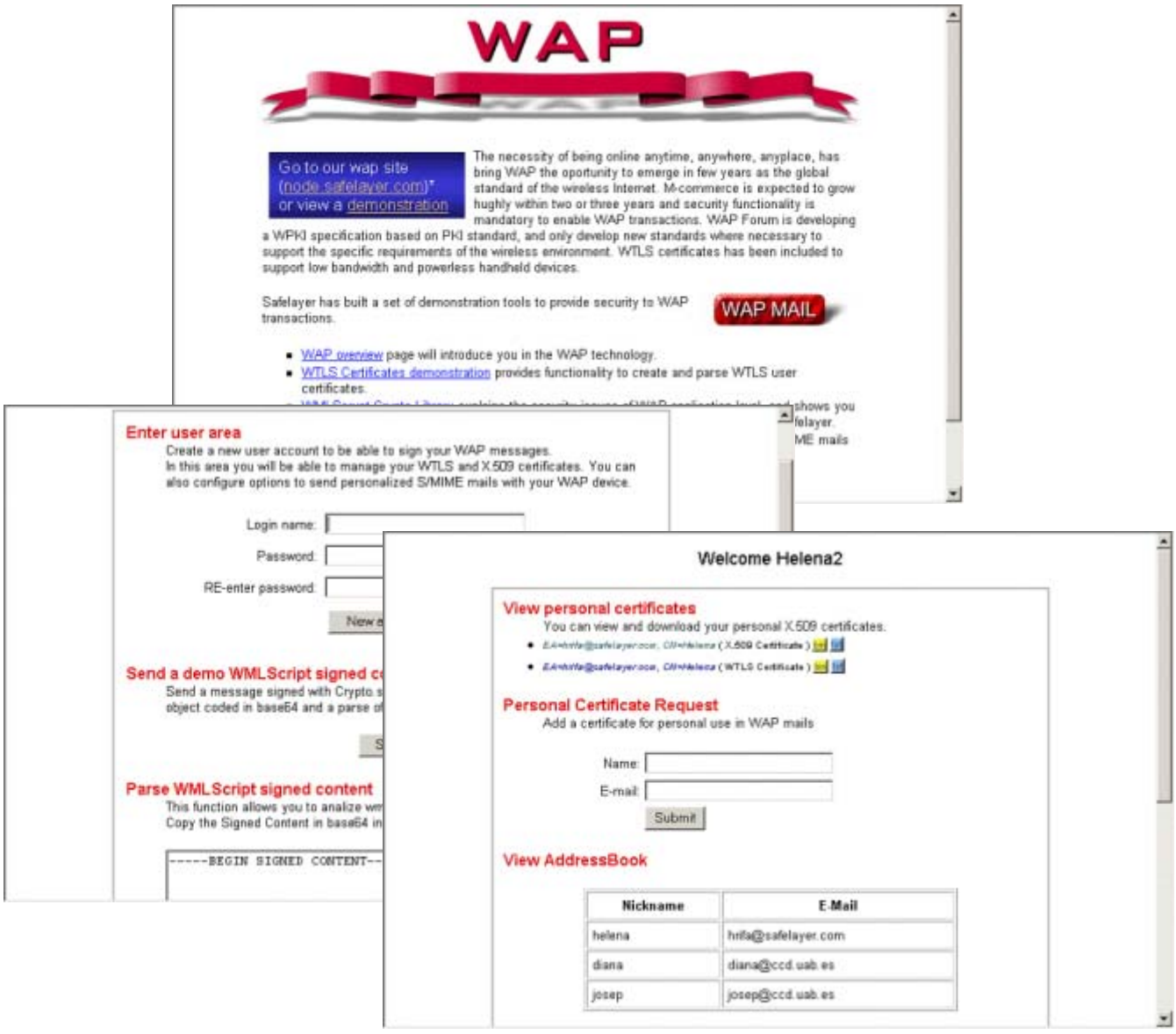

Figura 7: Interfaz WEB de wMail Secure Gateway

4. CONCLUSIONES

La tecnología WAP es aún muy nueva y las especificaciones del protocolo son muchas veces ambiguas y poco definidas. Las implementaciones que existen de productos con tecnología WAP no siguen exactamente las directrices marcadas por el Forum, haciendo que existan bastantes problemas de incompatibilidades. La parte de seguridad es una de las más nuevas y

de las que plantea más interrogantes. El hecho que no exista un protocolo extremo a extremo para hacer las comunicaciones seguras desde el móvil al servidor web preocupa de manera importante a la comunidad. Es por eso que se ha empezado a hablar de una migración hacia TCP/IP en la versión WAP 2.0. El lenguaje WML también es muy limitado y se propone hacer la translación a XHTML.

Aunque WAP tiene cada día más respaldo y es más conocido, también han empezado a surgir opiniones contrarias. Especialmente se critica que WAP es sólo un producto de márqueting y que la parte ingenieril se ha dejado mucho de banda.

Se ha intentado que WAP pudiera adaptarse en casi todas las redes existentes (CDPD, CDMA, GSM, iDEN, TETRA, DECT, SMS, USSD,...), incluso en redes obsoletas para los propósitos de WAP, como FLEX y REFLEX. Esto ha hecho incrementar innecesariamente la complejidad de la especificación.

Las redes de comunicaciones móviles se están estandarizando rápidamente hacia IP. Algunas de las redes más modernas como CDPD y Packet CDMA ya suportan IP nativo, y se espera que otras lo podrán hacer en un futuro próximo. Parecería mejor aceptar el IP como servicio estándar para el nivel de red e implementar protocolos altamente eficientes sobre esta capa.

El aspecto en el cual se ha centrado este proyecto, la seguridad en WAP, también tiene puntos débiles importantes. En particular se han encontrado posibles hoyos de seguridad en el protocolo WTLS, que aunque se ha adaptado del conocido TLS, no es exactamente lo mismo. Estas diferencias han provocado problemas como:

- Vulnerabilidad a los ataques de truncación de datagramas
- Ataques de mensajes extranjeros
- Ataques de fuerza bruta en algunas claves exportables

Además, el hecho de que WTLS y SSL sean incompatibles obliga a utilizar una pasarela para poder acceder a los recursos de Internet existentes, haciendo que la seguridad extremo-extremo entre el terminal móvil y el proveedor de contenidos sea imposible.

Es por todos estos problemas que Wap Forum está intentando reencaminar el WAP hacia un protocolo basado en IP y que soporte el lenguaje xHTML.

Después del dinero invertido para dar a conocer el WAP y con la gran cantidad de empresas interesadas en que este estándar siga adelante, parece bastante claro que WAP no puede desaparecer de un día para otro. Pero lo que sí es evidente es que WAP tal como lo conocemos hoy en día no tiene futuro. Wap Forum creará nuevas especificaciones y diseñará un nuevo estándar compatible con Internet, con más prestaciones para ofrecer servicios adicionales a aquellos usuarios que se conecten con redes de ancho de banda aceptable, con unas reglas más estrictas de cara a los fabricantes para evitar incompatibilidades de micronavegadores, y con la posibilidad de ofrecer servicios de seguridad extremo a extremo entre usuarios y contenido. Quizá este estándar no tendrá mucho que ver con el actual, pero después de las grandes campañas publicitarias que se han hecho de WAP, se trata de aprovechar que la población ya conoce este protocolo y ha depositado esperanzas en su funcionamiento.

5. IMPLEMENTACIONES

La pasarela de signatura digital implementada en este proyecto ha servido para mostrar la compatibilidad de la tecnología de clave pública de **Safelayer Secure Communications** en el mundo de los teléfonos móviles, y ha permitido que la empresa se pudiera posicionar como un punto de referencia en el mundo de la seguridad en WAP. La demostración de las funciones de firma digital publicadas en la WEB han servido para hacer pruebas de interoperabilidad con otras empresas del sector para analizar y solventar las deficiencias del estándar.

Asimismo, esta pasarela WAP/SMIME ha sido el prototipo inicial de nuevos proyectos en el campo de la seguridad en WAP conseguidos por **Safelayer**. **Safelayer** está desarrollando un proyecto (E-MTS II) junto con Amena y Microelectrónica Española, S.A. para realizar una maqueta de comercio electrónico con móviles (m-commerce) en el que se aplique la seguridad proporcionada por la tecnología PKI y se pueda pagar con el terminal inalámbrico. La maqueta que se desarrollará utilizará la pasarela WAP/SMIME para traducir los contratos de compra al formato estándar de Internet (PKCS#7). El piloto será una extensión del proyecto realizado ya que incorporará nuevas tecnologías no disponibles en el momento en que éste se desarrolló. Incorporará tecnología SWIM, por lo que el móvil será capaz de firmar sin tener que delegar esta función a un servidor de confianza. También utilizará la tecnología Push de WAP para enviar mensajes WML al móvil desde un servidor WEB. Con este proyecto aún se integran más los dos entornos de comunicaciones y se demuestra la convergencia de las tecnologías de la información y comunicaciones.