8. APLICACIÓN DESARROLLADA I

8.1 Introducción

EL objetivo de este proyecto consiste en firmar digitalmente facturas electrónicas almacenadas en un servidor WebDAV mediante un teléfono móvil con soporte J2ME utilizando Servicios Web XML. Esta firma deberá ser verificada por una aplicación fiable. En este caso, se ha utilizado la aplicación @firma de la Junta de Andalucía.

Como punto de partida, el servidor WebDAV ya se encuentra implementado. Este servidor se encarga de almacenar los documentos que debes ser firmados por el cliente, ya sean albaranes, facturas, etc., así como recoger y almacenar el fichero .p7 que recoge la firma digital realizada por el cliente móvil.

Previo al almacenamiento de la firma en el servidor, ésta debe ser verificada por una autoridad de confianza, que se encuentra previamente instalada en un servidor de aplicaciones.

Se trata de desarrollar los servicios web adecuados que permitan rescatar y devolver los documentos y la firma, respectivamente, al servidor. Para ello, el dispositivo móvil debe tener soporte J2ME y acceso a Internet, puesto que es necesario especificar la URL en la que se encuentran desplegados los servicios web necesarios para la aplicación.

En los siguientes apartados se explicará brevemente el desarrollo de la parte cliente y servidor, la interconexión entre ambos y los protocolos y servicios usados.

A continuación, se muestra un esquema que refleja la arquitectura de la aplicación desarrollada:

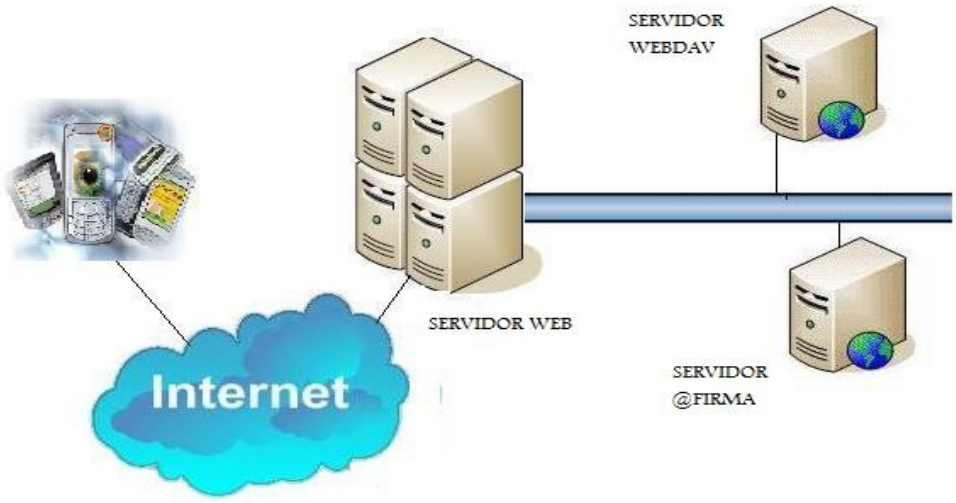

Figura 8.1. Arquitectura de la aplicación desarrollada

8.2 Desarrollo del servidor

8.2.1 Servidor Web XML

El proyecto implementa un servidor Web XML donde se encuentran desplegados los servicios web necesarios para acceder al servidor WebDAV. Es decir, los servicios web no son más que la simulación de un cliente Java que permite gestionar documentos del servidor WebDAV y estos servicios se encuentran a su vez desplegados en el servidor Web XML.

El servidor Web XML ofrece una interfaz necesaria a través de la cual se pueden ejecutar los métodos solicitados y devolver el resultado conveniente. Estos servicios web son invocados por el cliente móvil, que mandará los parámetros necesarios para realizar la llamada correctamente.

El servidor utilizado para poder desplegar los servicios web es el servidor de aplicaciones Apache Tomcat, al que se le ha añadido el módulo de Apache Axis. Se ha elegido dicho servidor por ser de software libre y uno de los servidores cuyo uso está más extendido. Su principal ventaja es su contrastada fiabilidad. Al estar escrito en Java permite ser ejecutado en cualquier sistema operativo que posea máquina virtual Java.

8.2.2 Comunicación entre servidor WebDAV y Servidor Web

La comunicación entre servidor WebDAV y servidor Web XML debe ser transparente al usuario. El cliente debe hacer una llamada al servicio web correspondiente, de forma que éste servicio web se comunique con el servidor WebDAV y devuelva o almacene los documentos solicitados, tras la previa autenticación del usuario. La comunicación entre ambos servidores se hará mediante el protocolo HTTP.

8.2.3 Comunicación entre servidor WebDAV y Servidor de Aplicaciones de @firma

La comunicación entre el servidor web y el servidor de aplicaciones @firma debe ser también transparente al usuario. Debe tratarse de una comunicación segura, puesto que al servidor donde se encuentra la herramienta de verificación de la firma, puede recibir peticiones donde viajen elementos importantes de la firma, como son el certificado digital de usuario. Por tanto, el protocolo de comunicación entre ambos se hará mediante HTTPS.

Un esquema que representaría la comunicación entre el cliente y los servidores sería el siguiente:

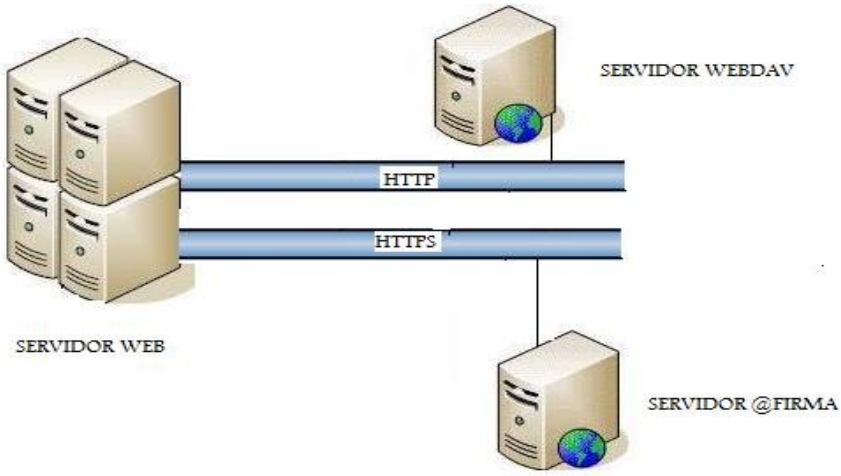

Figura 8.2. Protocolos de comunicación entre servidores

8.3 Desarrollo del cliente

El cliente móvil es el dispositivo que actúa como cliente consumidor de los servicios web. Para poder realizar la llamada a los servicios web, el dispositivo móvil debe poseer la interfaz JSR-172, para permitir la comunicación con los servicios web externos. Además, también debe poseer la interfaz JSR-75, que permite acceder al sistema de ficheros del dispositivo y tarjetas extraibles. Esta especificación es requerida para disponer de acceso al certificado de usuario, obtener y almacenar el fichero original y generar el fichero de firma PKCS7.

La especificación JSR-172 ya ha sido estudiada anteriormente en el capítulo 4 de esta memoria.

El formato de los documentos a firmar son .pdf, puesto que al tratarse de facturas y albaranes electrónicos, no deben ser modificados ante del proceso de la firma. Uno de los servicios web invocados permite descargar el fichero que se quiere firmar. No obstante, antes de iniciar el proceso de firma, es recomendable poder visualizar el documento con alguna aplicación del móvil que permita abrir documentos .pdf.

El formato devuelto por el proceso de firma es .p7, encapsulado en PKCS7. Dicho formato también ha sido documentado y explicado en el capítulo 4 de esta memoria.

8.4 Comunicación Cliente Móvil-Servidor Web

Los servicios Web permiten que el usuario se abstraiga de la comunicación, protocolos y datos intercambiados entre el cliente y el servicio web.

El servidor web ofrece al cliente la posibilidad de consumir cinco servicios web, que se explicarán con más detalle posteriormente. No obstante, los servicios web ofrecidos son los siguiente:

1. Autenticación con el servidor WebDAV.

2. Obtención de la lista de documentos existentes en el servidor WebDAV para ser firmados.
3. Obtención de los datos (contenido, nombre y fecha de última modificación) del documento seleccionado de la lista para ser firmado.

4. Obtención del hash del documento que se desea firmar, así como el registro del documento en @firma.

5. Custodia del fichero PKCS7 en el servidor WebDAV.

Los datos intercambiados entre el cliente y el servidor en los servicios web varían, obviamente, dependiendo del servicio web invocado. Así, la arquitectura de protocolo de cada servicio web cambiaría dependiendo del servicio. No obstante, todos seguirían la misma estructura hasta llegar a la última capa, que dependería de los tipos de datos intercambiados.

A modo de ejemplo, la arquitectura de protocolo del servicio web número 3 quedaría del siguiente modo:

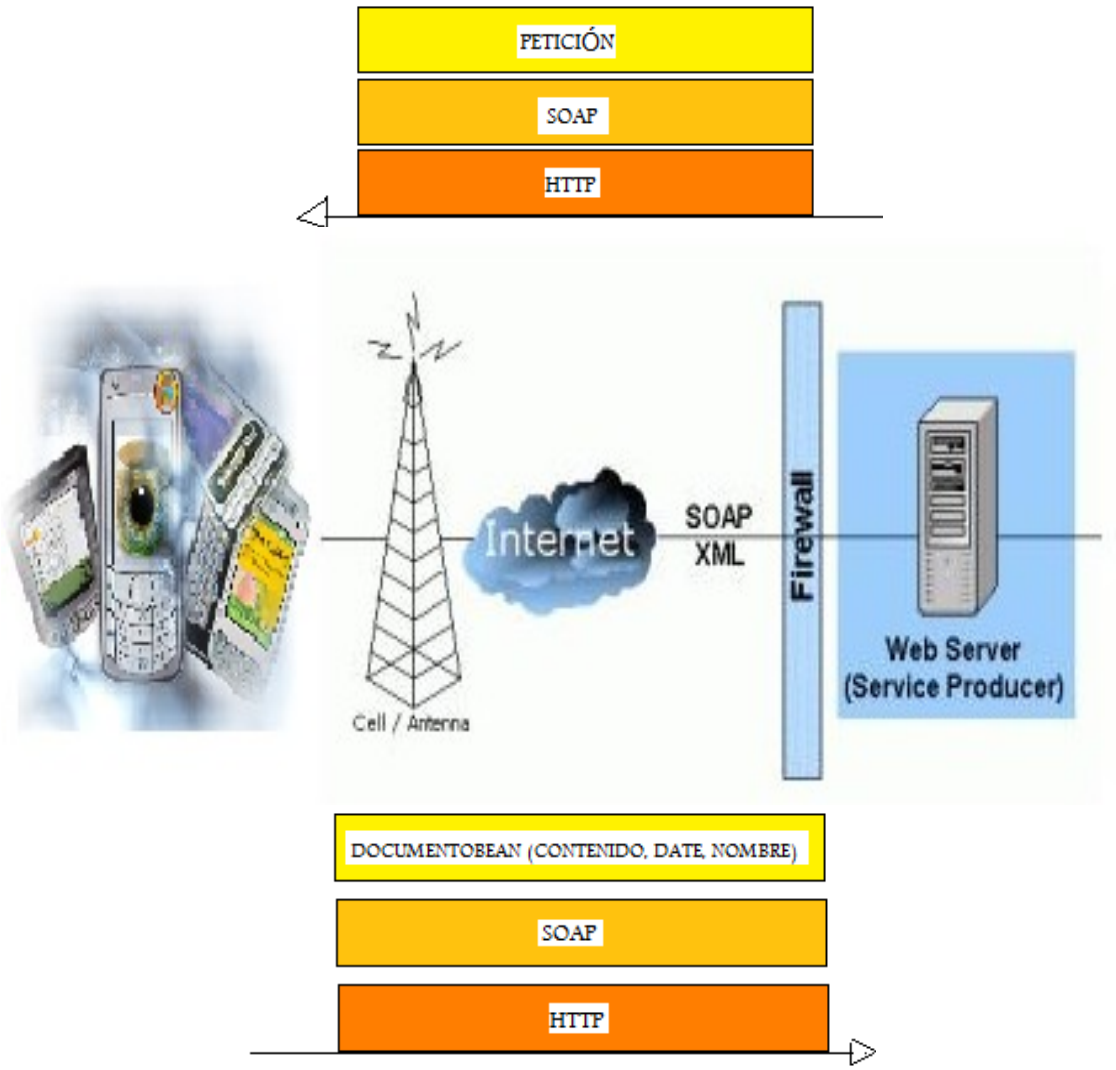

Figura 8.3. Arquitectura de protocolo del servicio web número dos

donde DocumentoBean representa una estructura con todos los datos correspondientes al documento elegido.

El servicio web número 3 devuelve la lista de documentos rescatadas del servidor WebDAV. Por tanto, la torre de protocolos quedaría del siguiente modo:

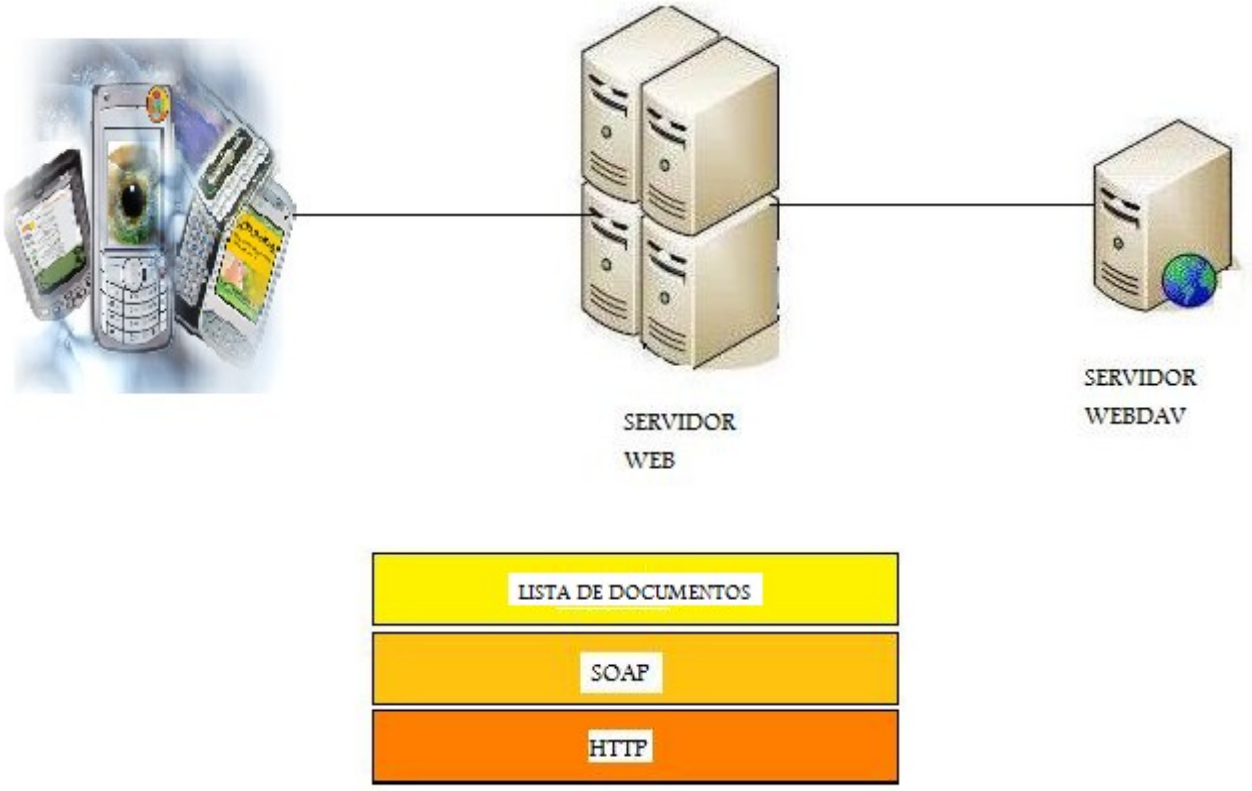

Figura 8.4. Arquitectura de protocolos de los servicios web

El resto de los servicios web seguiría el mismo esquema, pero la torre de protocolo de la respuesta cambiaría dependiendo de los datos intercambiados, que en el resto de servicios se trata de un String, representando distintas cosas dependiendo del servicio. Así, encontramos las distintas torres de protocolos:

Figura 8.5. Arquitecturas de protocolos del resto de los servicios Web

Antes de terminar este capítulo, es importante señalar que todos los String intercambiados van codificados en Base64, para evitar problemas de interpretación derivados.

En el capítulo siguiente, se explicará con más detalles todo lo relativo a los servicios web intercambiados.