1. INTRODUCCIÓN Y OBJETIVOS

El presente proyecto pretende ser una guía de iniciación a la implementación de la firma electrónica en dispositivos móviles. Por todos es sabido que los teléfonos móviles presentan ciertas limitaciones computacionales y de memoria. Por este motivo, cualquier solución adoptada debe tener en cuenta todas estas limitaciones.

En la actualidad, los avances en el campo de la tecnología móvil nos lleva a pensar en la gran posibilidad de servicios avanzados que se pueden ofrecer. Así, uno de los campos que puede beneficiarse ampliamente de estos servicios es el relativo al comercio electrónico móvil, cuyo principal objetivo es permitir a los usuarios realizar operaciones desde sus dispositivos con total seguridad y confianza.

En el marco de estos servicios seguros, surge la idea de la posibilidad de realizar firma electrónica en un dispositivo móvil. Un firma electrónica, se obtiene a partir de la aplicación de una serie de operaciones criptográficas en el documento que se va a firmar. Por este motivo, la firma electrónica debe satisfacer tres propiedades básicas:

1. Es relativa a un documento o a un determinado mensaje, y por tanto, no es extensible a otro documento o mensaje distinto.

2. Está asociada a la identidad del firmante y sólo ese firmante en concreto puede generar su firma particular.

3. Debe ser verificable públicamente, y por tanto, cualquier cambio o alteración debe ser detectado.

Por todo ello, es necesario disponer de un elemento identificador que permita identificar a un usuario concreto y de forma unívoca: es lo que se conoce como certificado digital del usuario. En el mundo digital, este certificado equivale al documento de identidad de la persona, y permite asociar una determinada clave a una identidad concreta. Así, será determinante para verificar que la clave usada para firmar un documento o mensaje pertenece a su identidad correspondiente.

La aparición de este proyecto surge en el marco del comercio electrónico orientado a las pequeñas y medianas empresas de determinados municipios. De esta forma, cada una de estas empresas, tiene la posibilidad de tener un espacio reservado en un servidor donde se encuentren todas las facturas y albaranes que se deseen firmar. El desarrollo de este proyecto, tiene como principal objetivo, permitir la firma electrónica de dichos documentos correspondientes a un usuario o empresa concreta desde un dispositivo móvil.

Los principales objetivos que se pretenden lograr son los siguientes:

1. Realización de firma digital por parte de un cliente móvil.

2. Desarrollo de servicios web necesarios para proporcionar al cliente móvil todas las aplicaciones necesarias, con el fin de liberarlo de cualquier carga extra.

3. Validación por algún organismo competente de la firma electrónica realizada.

4. Devolución de la firma realizada al servidor donde se encuentra el documento original.

Para cumplir todos los objetivos anteriores, ha sido necesario hacer un estudio preliminar de todas las opciones existentes en el mercado actual. Así, en el capítulo número 2, se presentan todas las opciones estudiadas a nivel general para la implementación de la firma electrónica en dispositivos móviles.

En el capítulo 3 se expone con una extensión moderada, todo lo relativo a la plataforma de desarrollo y ejecución Java J2ME, exclusivo para diseñar aplicaciones en dispositivos móviles. Dicho lenguaje proporciona perfiles y configuraciones diversas atendiendo a las distintas naturalezas de los dispositivos inalámbricos existentes en el mercado.

Como ya se ha comentado, es necesario liberar al teléfono móvil de la mayor carga posible. Para ello, se hace imprescindible el desarrollo de servicios web que permitan ser invocados por el cliente. Así, la llamada por parte del dispositivo móvil con los parámetros adecuados, devolverá aquéllo que se solicite. Para comprender mejor este tema, se presenta un estudio en el capítulo 4, explicando especialmente la invocación de dichos servicios en un dispositivo inalámbrico.

Además, para poder realizar la firma electrónica correctamente, es necesario poseer los conocimientos criptográficos adecuados. En el capítulo 5, se exponen los distintos tipos de cifrados y algoritmos existentes, los diversos formatos de firma electrónica reconocidos oficialmente, y certificados digitales.

La funcionalidad de este proyecto implica que los documentos que se deben firmar corresponden a facturas, albaranes,...electrónicos, todos ellos almacenados en un servidor donde cada usuario posee sus propios documentos. Más concretamente, el servidor donde se encuentran los documentos a firmar utiliza el protocolo WebDAV. Por ello, el capítulo 6 de esta memoria está dedicado al estudio de dicho protocolo, a los diferentes métodos que soporta para recuperar y devolver documentos al servidor, así como al inicio de sesiones independientes para cada usuario.

Uno de los objetivos principales de este proyecto, consiste en verificar que la firma realizada es correcta. Como ya se comentará a lo largo del desarrollo de esta memoria, ésto implica que la firma realizada se corresponda con los datos que se han firmado, que el certificado con el que se ha firmado sea válido, esté vigente y haya sido expedido por una autoridad certificadora y por último, que el usuario que haya firmado sea efectivamente el emisor de la firma. Para poder realizar todo lo anterior, se ha hecho uso de la plataforma de la Junta de Andalucía denominada @firma. Por este motivo, el capítulo 7 está dedicado exclusivamente al estudio de dicha plataforma, a los servicios que proporciona y a cómo utilizar dichos servicios.

Los siguientes capítulos, muestran el desarrollo de la aplicación de forma más detallada, correspondiente al desarrollo del cliente y del servidor, así como el escenario de pruebas realizado. Ésto corresponde a los capítulos 8 y 9.

En el capítulo 10 se establecen las conclusiones y los objetivos conseguidos, así como las líneas futuras de mejoras.

Por último, en los capítulos 11 y 12 se realiza un estudio del presupuesto y temporización,

respectivamente; y en el capítulo 13 se elabora una guía de instalación con los pasos seguidos para la instalación del cliente móvil y todo lo necesario para desarrollar los servicios web existentes en el servidor web.