COMUNICACIÓN TECNIMAP 2007

Nombre: Diana Caminero García

NIF: 50848600Q

Teléfono: 609120450

Correo electrónico: diana.caminerogarcia@telefonica.es

Organismo / Empresa: Telefónica Grandes Empresas

Puesto de trabajo: M2M y Negocios Transaccionales- Gerencia Marketing de Producto Móvil

Dirección de trabajo: Ronda de la Comunicación s/n. Distrito C. Norte 3, Plta 2ª. 28050 MADRID

Título de la comunicación: Firma digital en el Móvil

Resumen de la comunicación

Telefónica España, en su condición de empresa estratégica, ha venido trabajando en diversos proyectos hasta la fecha, invirtiendo y creando el entorno tecnológico necesario para facilitar el desarrollo de nuevas aplicaciones y servicios relacionados con la firma digital en el móvil. A tal fin, Telefónica España proporciona una plataforma de firma que hace posible el flujo de información y transacciones entre los usuarios móviles MoviStar y las empresas interesadas en los servicios de identificación y firma a través de certificados de firma electrónica.

NUEVO SERVICIO FIRMA MÓVIL DE TELEFÓNICA

Telefónica España es el Operador de telefonía líder en el mercado español, y cuenta con medios materiales, experiencia, conocimientos y cualificación técnica de sus recursos, en el sector de las Telecomunicaciones y en materia de implantación y desarrollo de proyectos relativos a la Sociedad de la Información.

Telefónica España quiere liderar el nuevo entorno digital, y para ello está comprometida en facilitar el desarrollo de los negocios, proporcionándoles servicios innovadores basados en las tecnologías de la información y la comunicación.

Telefónica España, en su condición de empresa estratégica, ha venido trabajando en diversos proyectos hasta la fecha, invirtiendo y creando el entorno tecnológico necesario para facilitar el desarrollo de nuevas aplicaciones y servicios relacionados con la firma digital en el móvil. A tal fin, Telefónica España proporciona una plataforma de firma que hace posible el flujo de información y transacciones entre los usuarios móviles MoviStar y las empresas interesadas en los servicios de identificación y firma a través de certificados de firma electrónica.

La novedad más reciente es el desarrollo por parte de Telefónica del servicio de ámbito internacional *Firma Móvil*, que proporciona a las empresas una herramienta para firmar digitalmente por medio del móvil en un entorno que garantiza la integridad, autenticidad y no repudio de las operaciones realizadas. Se trata por tanto, de un proyecto de especial importancia relacionado con la utilización de la firma electrónica en dispositivos móviles que cuenten con tarjeta SIM criptográfica, para procedimientos y comunicaciones administrativas dentro de la propia empresa y en sus relaciones con terceros.

La posibilidad de combinar los sistemas de seguridad propios de la telefonía móvil (en los que la tarjeta SIM funciona como módulo de identificación personal garantizando la privacidad y seguridad de las comunicaciones móviles) con los sistemas de PKI, proporciona un entorno de mayor seguridad que los sistemas convencionales. Su uso, por tanto, es más recomendable para entornos en los que se requiera un nivel de seguridad mayor, o en los que exista mayor riesgo de robo o pérdida de datos.

El servicio *Firma Móvil* está basado en *SIM Criptográfica*, en la que se generan y almacenan las claves, como dispositivo seguro de creación de firma. Se trata de un servicio que permite la realización de firma electrónica avanzada (vinculada al firmante de manera exclusiva y creada por medios que éste mantiene bajo su exclusivo control) y reconocible (basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma).

A tal fin, Telefónica proporciona una *plataforma de firma* que hace posible el flujo de información y transacciones entre los usuarios móviles MoviStar y las empresas interesadas en los servicios de identificación y firma a través de certificados de firma electrónica.

Para firmar digitalmente desde el móvil los usuarios sólo necesitan un certificado electrónico emitido por una *Autoridad de Certificación*, asociado a las claves generadas en su tarjeta SIM criptográfica.

Descripción General del Servicio Firma Móvil

El ***servicio Firma Móvil*** permite a las Grandes Empresas obtener transacciones de firma y/o autenticación de sus empleados, colaboradores, proveedores, clientes, y en general, cualquier usuario del que se requiera.

La empresa Gran Cuenta que contrate el servicio enviará a los usuarios finales solicitudes de firma y/o autenticación, a través de la red de Telefónica. Los usuarios pueden ser internos (empleados de la empresa) o externos (personal ajeno).

Para los usuarios finales del servicio, se trata de una forma de realizar operaciones con empresas basadas en ***certificados digitales*** mediante su móvil.

El usuario necesita disponer de una ***tarjeta SIM criptográfica***, que le será facilitada por la empresa que le ofrece los servicios de firma. El usuario será el que solicite la activación de la tarjeta criptográfica recibida, a través del CRC.

Además, deberá registrar al menos un certificado para su utilización desde el móvil. La empresa que le facilita la tarjeta criptográfica para la realización de transacciones es la que le indicará la forma de registrar el certificado requerido para ello. Este registro se realizará a través de la ***Autoridad de Registro*** indicada por la empresa (la Autoridad de Registro recoge los datos del usuario y cursa la petición de certificado hacia la ***Autoridad de Certificación*** correspondiente).

El ***servicio de Firma Móvil*** permite a las empresas obtener garantías de que la información no ha sido manipulada (integridad de los datos), de la autenticidad e identidad del firmante y del no-repudio de las transacciones realizadas por el usuario.

La tarjeta SIM criptográfica del usuario actúa como **dispositivo seguro de creación de firma**, puesto que el par de claves (pública y privada) se genera en la propia tarjeta, quedando almacenada de forma segura en la misma la clave privada, que nunca abandonará la tarjeta SIM. Esta circunstancia hace que se trate de firma electrónica avanzada (vinculada al firmante de manera exclusiva y creada por medios que éste mantiene bajo su exclusivo control). Además, si se emplea un certificado reconocido oficialmente, la firma realizada tendría el mismo valor que la firma manuscrita.

Cada par de claves generado por la tarjeta SIM del usuario podrá asociarse a un certificado digital, pudiendo disponer el usuario de varios certificados de la misma o distinta ***Autoridad de Certificación*** (emite los certificados de usuarios). Estos certificados son específicos para su utilización en el móvil.

Por tanto, un usuario podrá realizar operaciones de firma/autenticación con una o más empresas que le ofrezcan el servicio, empleando los certificados requeridos con cada una de ellas. Se trata de una forma de firmar o autenticarse digitalmente segura para el usuario (se requiere siempre la introducción de una clave de firma por parte del usuario).

No es necesario que las tarjetas SIM se inserten en terminales móviles especiales; el único requisito del terminal es que soporte mensajes cortos.

Este innovador servicio incorpora dos modalidades y por tanto, dos opciones contratables para la Gran Cuenta: ***Firma Móvil sin Validación (Modelo A)*** y ***Firma Móvil con Validación (Modelo B)***.

La opción ***Firma Móvil sin Validación*** permite a la empresa Validar los certificados digitales móviles utilizados contra la Autoridad de Certificación pertinente y Verificar las firmas recibidas, a través de sus propios medios y según su propia política de PKI.

El ***Servidor de Firma Móvil*** es un servidor específico del servicio que encamina las solicitudes de firmas hacia los usuarios finales y entrega las firmas realizadas a la empresa. La infraestructura de Validación de Certificados y Verificación de Firmas estará por tanto en la empresa.

Mediante la opción ***Firma Móvil con Validación***, Telefónica se encargará de Validar los certificados empleados y de Verificar las firmas realizadas por los usuarios finales. En este caso, Telefónica ofrece a las empresas la posibilidad de disponer de un servicio de firma móvil sin necesidad de disponer de la infraestructura PKI necesaria para verificar las firmas recibidas, ni establecer acuerdos con las Autoridades de Certificación para la validación de los certificados.

Los beneficios derivados de la utilización del ***Servicio Firma Móvil***, son el incremento de la seguridad en operaciones realizadas desde el móvil, optimizando los procesos de la empresa y abriendo nuevas oportunidades de negocio facilitando el desarrollo de nuevas aplicaciones en movilidad.

Los elementos principales de esta arquitectura son:

- ***Tarjetas SIM criptográficas***: tarjetas que disponen de un criptoprocesador y de una aplicación Java Card que permite cifrar datos mostrados en la pantalla del terminal cuando el usuario introduce un PIN. El criptoprocesador es la implementación hardware que acelera el procedimiento de cifrado. Las claves del usuario se generan en la tarjeta SIM y los procesos de firma se realizan en la aplicación criptográfica de la propia tarjeta.

- ***Servidor de Firma Móvil***: plataforma del servicio que solicita la firma de unos datos al usuario bajo demanda de la aplicación final del cliente, y devuelve los datos firmados a dicha aplicación o bien el rechazo de dicho usuario a firmar lo solicitado.

- ***Red GSM/GPRS/UMTS de TME***: la comunicación entre el Servidor de Firma Móvil y las tarjetas SIM se realiza a través de SMSs binarios, de manera universal para todo el parque de terminales.

- ***Prestadores de servicios de Certificación***: existen distintos actores según las funciones que realicen:

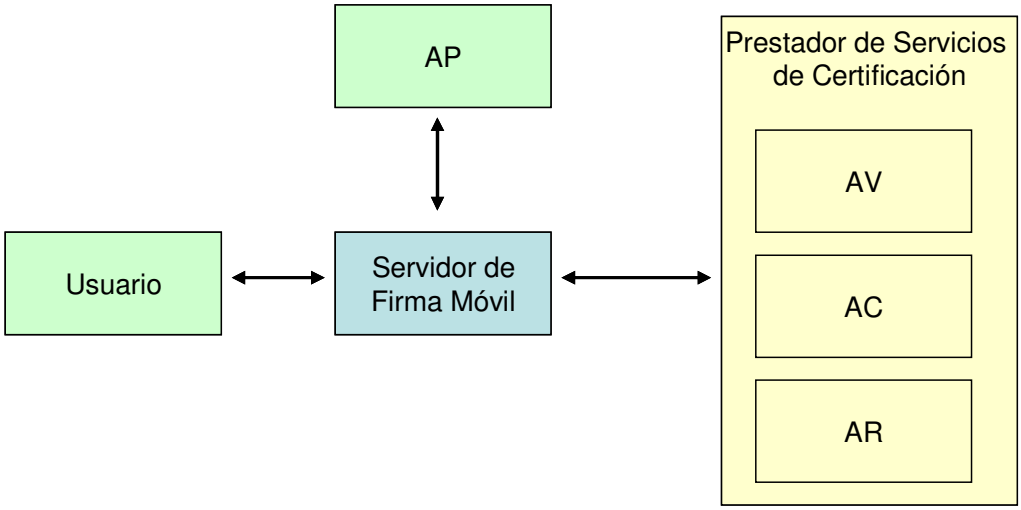
    - **Autoridad de Certificación**, entidad que emite y garantiza la validez y unicidad de los certificados móviles de usuarios y entidades, actuando como entidad de confianza.

    - **Autoridad de Registro**, implementa el proceso de registro establecido en la política de certificación de la Autoridad de Certificación con la que se integra. Se encarga de registrar los datos del usuario y progresar la solicitud hacia la Autoridad de Certificación para que emita el certificado. Comprueba, en ocasiones presencialmente, la validez de los datos de identificación del solicitante.

    - **Autoridad de Validación**, provee de un servicio de validación de la vigencia de los certificados.

- ***Red Internet***: La conexión entre la red de TME y los servidores del cliente se realiza a través de Internet.

- ***Aplicaciones de firma del cliente***: El último elemento implicado en la arquitectura del servicio son las aplicaciones del cliente, que realizan solicitudes de firma a los usuarios móviles a través del Servidor de Firma Móvil, de acuerdo a su lógica interna. Las aplicaciones del cliente se comunican con el Servidor de Firma Móvil a través de web-services para invocar las funcionalidades del servicio.



El proceso de firma para el usuario final desde su móvil es sencillo e intuitivo:

a) La aplicación de firmas de la empresa detecta la necesidad de que un usuario realice la firma de un documento o transacción concreta, para lo cual envía al Servidor de Firma Móvil de Telefónica la solicitud de firma, indicando el número de móvil del profesor.

b) El Servidor de Firma Móvil de Telefónica remite al usuario la solicitud de firma. El usuario recibe en su móvil un mensaje indicándole que firme el documento concreto o autorice determinada acción. En la pantalla de su terminal visualiza el texto que tiene que firmar, de manera que el usuario firma lo que está viendo.

c) El usuario acepta la firma en su móvil e introduce para ello su PIN de firma (se trata de una clave selecciona por el usuario que sólo él conoce y que le da acceso a las funcionalidades criptográficas de la tarjeta SIM). Dentro de la tarjeta SIM criptográfica se realiza la operación de firma (calcula el hash del texto y lo cifra con la clave privada del usuario).

d) La tarjeta SIM envía la firma al Servidor de Firma Móvil de Telefónica y éste a la aplicación solicitante.

Valimo, proveedor finlandés de la plataforma de firma móvil, es líder del mercado de firma móvil, con amplia experiencia en lanzar servicios de firma móvil en varios países (Finlandia, Italia, Noruega, Eslovenia, Lituania, Turquía…) y con el hito de haber desarrollado el primer servicio basado en el estándar del ETSI de firma entre operadores y entre países. Así Telefónica se pone a la cabeza en toda Europa con el lanzamiento de la firma móvil y en el desarrollo y adopción de los estándares de la industria.

Aplicación empresarial:

La realización de firmas móviles en SIM proporciona oportunidades:

- en procesos en los que ya está implementada la firma electrónica en el entorno PC, la firma desde el móvil permite su realización en cualquier momento y lugar y con mayores garantías que los certificados SW en el entorno PC, al no poderse extraer las claves privadas de la SIM.
- en procesos en los que no está implementada la firma electrónica y que se producen en un entorno de movilidad, obteniendo una mayor eficiencia y facilidad de utilización.

- como complemento a operativas realizadas en entorno PC, en las que el móvil aporta un mayor nivel de seguridad a la identificación y firma del usuario

Las aplicaciones del servicio de *Firma Móvil* para las empresas y usuarios son múltiples, destacando:

* Firma digital para todo tipo de documentos digitales, como autorizaciones, validaciones de *workflows* (nóminas, ausencias, vacaciones, notas de gastos…), voto electrónico, multifirmas, firma de contratos...

* Identificación ante un acceso restringido, como acceso a Intranets, a información confidencial, a un servidor determinado, a aplicaciones específicas…

El servicio de *Firma Móvil* constituye una solución de firma completa e integrada que se adecua a las necesidades de seguridad, disponibilidad, rapidez, flexibilidad, usabilidad y modelo de negocio en los diferentes entornos. Los campos en los que la utilización de la firma digital móvil es más evidente, son Administraciones Públicas, Entidades Financieras, Servicios o Sanidad Privada.

Ejemplos prácticos:

Así lo entienden numerosas empresas que ya están aplicando en sus procesos internos o bien, en sus procesos con proveedores, agentes, clientes, las ventajas del servicio de *Firma Móvil* de Telefónica.

Para la Entidades Financieras, la implementación de la firma en el móvil supone un método seguro de identificación de sus clientes ante la banca en Internet, de manera que el usuario entra en la página Web y firma desde el móvil el acceso al portal seguro; sustituyendo a métodos tradicionales de usuario y contraseña.

También es posible la realización de operaciones bancarias identificadas de alto riesgo o con necesidades de seguridad y no repudio, como autorización de transferencias de importe elevado, mediante el certificado del usuario asociado a su tarjeta SIM criptográfica.

La *Universidad de Murcia*, especialmente volcada en el desarrollo tecnológico y en el despliegue de servicios telemáticos seguros apoyados en una infraestructura de administración electrónica propia, ofrece ya a los profesores docentes la posibilidad de firmar determinados flujos electrónicos desde su teléfono móvil. Un ejemplo es la firma de actas digitales, facilitando que los profesores no tengan que presentarse físicamente en las secretarías de los centros académicos a entregar las actas firmadas manuscritamente y permitiendo que los estudiantes reciban sus notas finales con mucha mayor rapidez. *UMU* tiene previsto "movilizar" otras aplicaciones de firma digital desplegadas en sus sistemas, incluidas los que se dirigen específicamente al alumnado.

Ventajas del Servicio Firma Móvil:

Las ventajas del servicio ***Firma Móvil*** son:

- Permite al cliente ampliar las posibilidades de la firma electrónica en aplicaciones que ya la utilizan, realizándolas también en entornos de movilidad.
- Incrementa la seguridad de las transacciones de firma realizadas en entorno PC con certificados SW, ya que la tarjeta criptográfica ofrece mayores garantías.
- Posibilita la realización de operativas en movilidad, que hasta ahora no eran abordables por sus altos requisitos de seguridad, confidencialidad o no repudio.
- Complementa operativas realizadas en otros entornos, como el PC, en los que el móvil aporta un mayor nivel de seguridad a la identificación y firma del usuario.

Al posibilitar la realización de firmas y autorizaciones a los usuarios, estén donde estén, se produce:

- Mejora en los procesos operativos y flujos internos de la empresa.
- Reducción de costes

- Nuevas oportunidades de negocio
- Mejora del servicio al cliente final
- Incrementa la productividad de la Empresa

Máxima **flexibilidad del servicio**, distintos modelos según las necesidades requeridas por la GC:

- La empresa puede decidir si realizar la verificación de firmas y validación de la vigencia de los certificados, o bien, delegar estas funcionalidades en Telefónica.
- MultiCA, el servicio se adapta a la Autoridad de Certificación requerida por el cliente.

A un **coste razonable**. Propone un modelo de facturación adaptado a las necesidades de las GGCC y flexible, de manera que:

- La GC puede asumir el coste del servicio haciendo que no tenga impacto para el usuario final y propiciando la utilización del servicio.
- O bien, la GC puede optar por que sea el usuario final el que asuma el coste de las transacciones de firma que realice.
- Favorece la adopción del servicio, de forma que si una línea no realiza transacciones de firma no se factura por nada por ello.
- Descuento por volumen: cuanto mayor número de transacciones de firma realice el cliente, menor será el precio por transacción.
- Independiza al usuario del coste de las comunicaciones necesarias para cursar una transacción de firma, de manera que el concepto facturable es la transacción en sí misma, sea cual sea el número de SMSs empleados en la misma.