CERTIFICACIÓN MÓVIL Y OPERATIVAS AVANZADAS DE SEGURIDAD

Gloria V.Alamillo Blanco
Coordinador del Proyecto
Telefónica Móviles España
Pza Independencia 6, 5ª Planta

Leticia Lopez Domingo
Coordinador del Proyecto
Telefónica Móviles España
Pza Independencia 6, 5ª Planta

Gloria V.Alamillo Blanco
Leticia Lopez Domingo

Palabras clave

PKI – Public Key Infrastructure.

Resumen de su Comunicación

La actual penetración de los dispositivos móviles en el mercado, así como la proliferación de las aplicaciones y servicios móviles en los distintos ámbitos privados, públicos y empresariales de nuestra sociedad , hace que a día de hoy el nivel de exigencia hacia el canal móvil como medio transaccional sea muy similar al existente a través de PC, de forma que ambos canales se sitúan en muchos casos a un mismo nivel operativo y funcional, diferenciándose en el grado de ubicuidad proporcionado por el canal móvil , que es a su vez su principal valor añadido.

La necesidad de que las transacciones telemáticas se desarrollen en un entorno seguro se extiende a la movilidad, y con ello, se hace necesario el uso de certificados digitales y operativos de firma digital desde dispositivos móviles, quedando garantizado el cumplimiento de propiedades fundamentales como la autenticación, confidencialidad, integridad y no repudio de las operaciones.

A través del proyecto de Certificación Móvil se ha conseguido desarrollar una serie de capacidades avanzadas de gestión y uso de certificados en movilidad, como la firma digital y la generación de sobres digitales, que cumplen con los estándares de seguridad digital vigentes (PKI) y en atención a las del parque de terminales móviles comercializado por TME. Los resultados del proyecto están siendo utilizados en el desarrollo de aplicaciones y servicios avanzados en los que la seguridad es un factor fundamental. Buena prueba de ello ha sido la integración de las capacidades de firma digital y gestión de certificados en aplicativos de votación y participación a través del terminal móvil y la adaptación de dichas capacidades al futuro DNI-e.

Gloria V.Alamillo Blanco
Leticia Lopez Domingo

CERTIFICACIÓN MÓVIL Y OPERATIVAS AVANZADAS DE SEGURIDAD

1. Introducción

En la actualidad, estamos asistiendo a una expansión importante en la implantación y uso de la firma digital en distintos entornos. Son muchos los flujos de operaciones que actualmente precisan de un procedimiento de firma digital avanzada por el cual se asegure la acreditación e identificación de las partes, la confidencialidad y privacidad entre las mismas, la autentificación de los contenidos y la garantía de no repudio, entendida como la imposibilidad de que ninguna de las partes pueda negar la operación.

La consolidación de estándares de firma digital, y en especial los relativos a infraestructura PKI (Public Key Structure), ha permitido que las complicadas soluciones de firma digital utilizadas casi exclusivamente en entornos de administración pública, hayan evolucionado y se hayan simplificado permitiendo el acceso de corporaciones y empresas de tamaños más reducidos a soluciones de firma digital que cubren necesidades específicas de la empresa, tanto en sus flujos internos, (empleado-empleado, directivo-empleado, directivo-directivo, etc.) como en su relaciones externas (proveedores, suministradores, empresas de servicios, administración pública y , por supuesto, cliente final)

En la actualidad, la mayoría de las soluciones de PKI establecidas, están dirigidas al entorno de PC, desde el cual se pueden realizar conexiones seguras o firmar y verificar documentos a través de los certificados disponibles en las aplicaciones del ordenador (ej. Repositorio de certificados de Microsoft) , o accesibles a través de dispositivos externos (diskette, token USB, tarjetas criptográficas,etc).

El importante crecimiento tanto de clientes que, cada vez más, hacen uso de dispositivos móviles tales como teléfonos y PDAs, así como el gran auge de servicios y aplicaciones desarrollados para estos terminales, hacen que tanto los grandes fabricantes de dispositivos móviles como los proveedores de servicios, comiencen a preocuparse por desarrollar y poner en marcha tecnologías que solucionen los actuales problemas de seguridad.

Con el proyecto de Certificación Móvil , Telefónica Móviles pretende extender el actual uso de la infraestructura PKI hacia terminales móviles, de forma que las entidades dispongan de un nuevo canal de acceso sobre el cual realizar operaciones relacionadas con el uso de la firma digital de acuerdo a estándares PKCS# , que aseguren la integridad del nuevo canal con las actuales infraestructuras PKI disponibles en la empresa, teniendo en cuenta las particularidades en cuanto a capacidad de proceso y características de almacenamiento propias del entorno de movilidad.

El objetivo fundamental, consiste en llevar a los terminales móviles las mismas propiedades de seguridad mediante certificados de usuarios de las que un usuario final dispone a través de un PC de escritorio.

Volver

Gloria V.Alamillo Blanco
Leticia Lopez Domingo

2.- Firma Digital en los procesos de e-Administración. El DNI digital.

Desde hacia varios años, la Administración está llevando a cabo diversas iniciativas dirigidas a crear la denominada Administración Electrónica. Bajo este paraguas se engloba la realización de todos los trámites administrativos (tanto internos como externos) a través de medios telemáticos, lo que facilita el contacto con la administración y contribuye a flexibilizar y mejorar la eficiencia de los procesos.

Buen ejemplo de ello, es el Plan de Modernización Tecnológica de la Administración Pública 2004-2007, conocido como Plan Conecta, está destinado a conectar administraciones y personas, mediante la reducción de la burocracia y la eliminación de trámites y esperas injustificadas. El proyecto cuenta con un presupuesto de 84 millones de euros en tres años, destinado a 'reinventar la administración desde la tecnología'.

En el desarrollo de estos proyectos tiene especial mención la implantación y uso de la firma digital, como único medio que otorga validez a las operaciones, tanto hacia las administraciones como ante una tercero o autoridad competente. A través de un sistema de clave pública (PKI) se comprueba que el documento o tramitación ha sido firmado por quien lo ha mandado y que además no ha sido manipulado durante el proceso de transmisión.

Sin embargo, la implantación de este tipo de sistemas en la administración está siendo lento debido a la existencia de diversas barreras, técnicas, económicas y políticas. En España el principal proveedor es la Fábrica Nacional de Moneda y Timbre y hasta ahora, apenas se han superado los 700.000 certificados. Toda esta situación podría cambiar en el corto plazo. Durante este año 2006, verá la luz el DNI digital, un documento muy esperado con el que la Administración pretende impulsar la Sociedad de la Información y el uso de Internet.

En los últimos meses, se ha venido hablando de la llegada del nuevo Documento Nacional de Identidad (DNI) que hará su aparición a comienzos de 2006. Su puesta en funcionamiento resulta un proyecto muy anhelado, pues su nacimiento se vislumbró en 1999 dentro del Plan Info XXI para el desarrollo de la Sociedad de la Información. Uno de sus objetivos principales era el de «facilitar una identidad digital a todos los ciudadanos de modo que el DNI sirva para identificarse tanto en un mundo físico como virtual».

Estamos pues en un punto de inflexión en la implantación y uso generalizado de la firma digital. La seguridad se hará presente en cualquier tipo de transacción que se realice a través de medios telemáticos (fijos y móviles), de forma que la firma digital tendrá la misma validez jurídica que la firma gráfica. La implantación del carnet de identidad electrónico, además de proporcionar nuevas utilidades, supondrá un paso importante en el desarrollo de las Nuevas Tecnologías y la Sociedad de la Información en nuestro país.

De todo lo expuesto, se desprende la necesidad de analizar las aplicaciones y el uso de los certificados digitales y la firma electrónica en el entorno de la telefonía móvil para garantizar la confidencialidad, integridad, autenticidad y no repudio de las operaciones realizadas a través de dicho terminal móvil.

3.- Aplicaciones y Servicios de Referencia

Al llevar los desarrollos realizados a estos entornos reales se consiguen las siguientes ventajas competitivas:

- Se dispone de una versión de aplicaciones existentes en un entorno móvil, lo cual ofrece un valor añadido al usuario final.

- Es posible acceder a servicios básicos del aplicativo desde distintos entornos, lo que flexibiliza el wor-

Volver

kflow.

• La securización de las transacciones electrónicas es indispensable para generar confianza y aceptación entre los usuarios finales.

• Se dota de características de rapidez y eficacia a los servicios existentes.

A continuación se muestran algunos de estos escenarios y el actual estado de implantación del servicio.

Concursos públicos Gobierno de Aragón

El Gobierno de Aragón posibilita la presentación telemática de ofertas a concursos públicos, de manera que a través de Web, y con conexiones seguras, las empresas pueden presentar sus propuestas.

Con el fin de hacer el sistema multicanal, y permitir que un usuario desde cualquier lugar y en cualquier momento pueda acceder a esta funcionalidad ofrecida por el Gobierno de Aragón, se ha realizado una prueba de concepto por la cual se trataba de dotar al sistema actual de movilidad, teniendo muy en cuenta los requerimientos relacionados con la seguridad e integrando las capacidades de certificación móvil desarrolladas (conexión https, firma digital del formulario, etc).

Servicio de validación de Ausencias

La Universidad de Murcia dispone de una aplicación multiservicio de gestión de recursos humanos llamada KRON. Esta aplicación funciona en la intranet de la Universidad y dispone, de entre sus muchas características, de un módulo de validaciones electrónicas mediante certificados de usuario. Este módulo permite la realización de dos acciones básicas

- Solicitar una ausencia por parte de un trabajador
- Validar o desestimar una solicitud de ausencia por parte de uno o varios supervisores.

Aplicando los desarrollos de certificación móvil, a este servicio ya existente en la Universidad de Murcia, se le ha dotado de un acceso móvil a través del cual es posible realizar la operativa completa de solicitud y validación de ausencias con plena confianza hacia las partes (co-firma digital)

Cliente de Voto Móvil

En colaboración con la empresa Scytl S.L, empresa proveedora de soluciones de e-Voto a través de Internet seguras y confiables, se ha desarrollado un proyecto por el cual ha sido posible ampliar y fortalecer su actual oferta de productos de votación remota (Juntas Generales de Accionistas, voto parlamentario, participación ciudadana, etc) mediante la creación de un cliente móvil de votación que basa su operativa fundamental en los desarrollos de seguridad de Telefónica Móviles España.