VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
www.tecnimap.com
Ponencias

Proyecto FIRMA

Gerard Cristòfol Roig
Consultor y jefe de proyectos en Tecsidel
Alberto Cuesta Escribano
Licenciado en Informática por la Universidad Politécnica de Madrid.

1 Introducción

El siguiente comunicado pretende mostrar un caso real de aplicación de tecnologías avanzadas de seguridad para resolver un problema real: las transacciones de alto valor en Internet.

1.1 Planteamiento del problema

El uso del comercio electrónico en España está en crecimiento, sin embargo ese crecimiento se está desarrollando a un ritmo lento. En parte, es debido a aún elevado coste de las comunicaciones y de los accesos a Internet; pero en parte se debe a la desconfianza que existe en los sistemas de seguridad actuales.

A un ciudadano, acostumbrado a ir a su tienda habitual, elegir un producto que puede ver, manipular y probar antes de comprarlo, y cuando decide hacerlo paga y se lleva su producto bajo el brazo, le es muy difícil comprar por Internet, cuando no puede ni probar el producto ni llevárselo, teniéndose que fiar de un vendedor al que ni siguiera conoce. Si trasladamos el problema a un entorno empresarial, el problema es aún mayor, pues no existe una ley que respalde el uso de tecnologías avanzadas de seguridad para realizar transacciones de alto valor en la red.

Debido a estos problemas, el Ministerio de Ciencia y Tecnología planteó un ambicioso proyecto que tuviera en cuesta no sólo los últimos avances tecnológicos, sino también el respaldo de la ley: el denominado Proyecto Firma.

1.2 Objetivos a cumplir

El Proyecto Firma tiene dos objetivos principales:

- Fomentar el uso del comercio electrónico en transacciones de alto valor: desarrollar un sistema que permita la gestión segura de títulos cambiarios desde Internet utilizando firma electrónica avanzada y siguiendo la legislación y, en la medida de lo posible, los procedimientos actuales.
- Estudiar la adecuación de la legislación y los procedimientos actuales a la nueva propuesta tecnológica: Modificar las leyes que fueran necesarias para que el uso de Internet en estas transacciones estén recogidas en las mismas.

Como ya se ha comentado, el desarrollo de sistemas de pago en Internet seguros, fiables y con respaldo legal es uno de los puntos clave para el crecimiento del comercio electrónico. Para la aceptación de los nuevos medios por parte de los usuarios resulta necesario que se produzcan avances en las dimensiones tecnológica, legal y social.

Para este propósito, el Ministerio de Ciencia y Tecnología, a través de su iniciativa PISTA, conduce la construcción de una plataforma segura que permita operar con títulos cambiarios electrónicos: el proyecto FIRMA. Donde converjan tecnología y marco jurídico para que el comercio electrónico sea socialmente aceptado.

2 Proyecto FIRMA

El proyecto firma pretende trasladar el uso de Títulos Cambiarios tradicionales en papel, como medios de pago en transacciones de alto valor, en Títulos Cambiarios Electrónicos (TCEs). La idea es buscar un formato electrónico capaz de satisfacer los requisitos operacionales de uso y seguridad, a la vez que legales.

En el Proyecto se realizará la gestión de los siguientes títulos cambiarios:

- Letra de cambio
- Cheque
- Pagaré
- Recibo

2.1 Requisitos Tecnológicos

Los requisitos tecnológicos para desarrollar un entorno seguro se resuelven mediante una infraestructura de PKI . Una PKI es un conjunto de políticas, prácticas, estándares y leyes que emergen de la criptografía asimétrica, concepto esencial de la firma-e.

Apoyadas en una PKI, las transacciones en la red garantizan la seguridad y ofrecen las prestaciones de autenticación, no-repudio e integridad de los datos.

La autenticación es necesaria para que en una transacción proveedor y comprador puedan comprobar que son quienes dicen ser. No-repudio implica que las transacciones realizadas comprometen a todos los participantes en la misma de modo que no pueden rechazarla. Y, por último, la integridad de los datos se refiere a la imposibilidad de alterar los documentos que forman parte de todo el proceso.

2.2 Arquitectura en tres capas

El diseño de la solución para el uso de títulos cambiarios electrónicos contempla la siguiente arquitectura en tres capas.

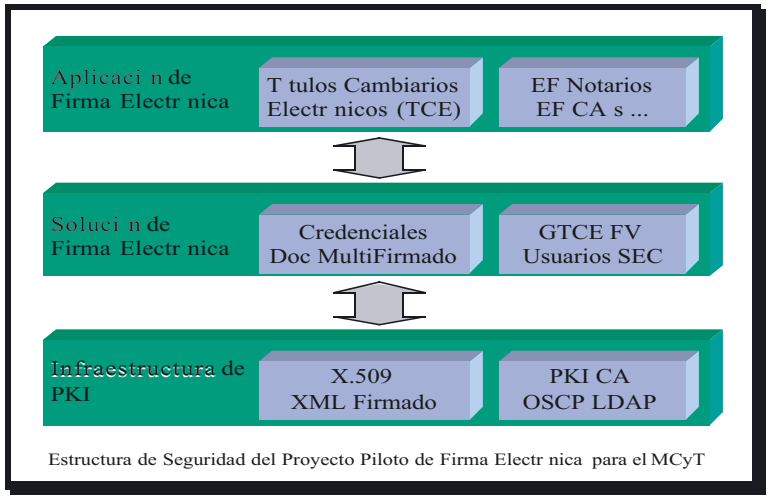

Figura : Arquitectura de la solución

La primera capa, Aplicación de Firma Electrónica, implementa la solución funcional del sistema. En esta capa hablaremos de Títulos Cambiarios Electrónicos (TCEs), que van a ser Cheques, Letras, Pagarés y Recibos. Dichos títulos se definen y se crean a este nivel.

La segunda capa, Solución de Firma electrónica, es la encargada de ofrecer servicios de seguridad a la capa superior. A este nivel hablaremos de Documentos Electrónicos Firmados (DEF). Los servicios de seguridad a ofrecer incluyen firma electrónica de Títulos, almacenamiento seguro de los mismos, pagos y cobros de las cantidades y transmisión o endoso segura de títulos. Esta capa ofrecerá los servicios de seguridad apoyándose en la última capa o capa de Infraestructura de PKI.

La última capa, Infraestructura de PKI, es la encargada de ofrecer los mecanismos necesarios para implementar las funcionalidades de Identificación, integridad, no repudio y privacidad, es decir, me proporcionará los certificados digitales.

2.3 Actores de la solución

Para implementar toda la funcionalidad, tanto de títulos como se seguridad, el diseño contempla los siguientes actores:

Usuarios

Entendemos por usuarios aquellas personas físicas o jurídicas que son sujetos de los derechos y / o obligaciones derivadas de los títulos cambiarios electrónicos.

Gestora de Títulos Cambiarios Electrónicos (GTCE)

Es la entidad encargada de la gestión de títulos. Será la encargada de realizar cualquier operación sobre los títulos:

- Creación de títulos
- Almacenamiento de títulos
- Transmisión de títulos
- Gestión del pago con las entidades finales

También se delega en esta entidad las funciones de interacción con el usuario, tales como:

- Facilitar la interacción del usuario con su cartera de TCE mediante una interfaz web.
- Llevar a cabo el control de acceso de usuarios utilizando firma electrónica avanzada.

Fuente de Verdad (FV)

La FV es una aplicación informática distribuida que garantiza las operaciones de TCE realizadas desde las GTCEs. En caso de accidente o de un poco probable uso perverso de la GTCE, la Fuente de Verdad es la que va a proporcionar toda la traza de un título.

Entre sus funciones, destacamos:

- Traza de las operaciones realizadas sobre los títulos.
- Proporcionar un directorio global de TCEs
- Proporciona la unicidad de los títulos.
- Realiza el registro de todas las operaciones de los TCE.
- Desde un punto de vista puramente jurídico, la FV es el elemento de resolución de conflictos sobre cualquier característica de un título.

Entidades financieras

Las entidades responsables de materializar las operaciones financieras necesarias para llevar a cabo los distintos procesos de los títulos cambiarios.

Entidad de Timbrado

Entidad que proporciona ejecutividad a las letras de cambio , proporcionando . Esto es, proporciona un identificador único para el documento (timbre).

Infraestructura de Clave Pública (PKI)

Conjunto de aplicaciones informáticas que permiten la firma electrónica avanzada.

Destacaremos las siguientes:

<u>Autoridad de Certificación (CA)</u>

Es la encargada de asegurar la identidad de los usuarios y entidades que intervienen en los distintos procesos de los TCE mediante Certificados Digitales, debiendo cumplir los requisitos necesarios para ser prestador de servicios de certificación y emisión de certificados reconocidos según el Real Decreto 14/1999.

Autoridad de Registro (RA)

Su función principal es la de recibir las solicitudes de certificación, bien para una petición de firma de certificado (CSR o Certificate Signing Request) o para proporcionar los datos identificativos necesarios para validar un certificado.

Entidad de Sellado de Tiempo

Es la encargada de proporcionar sellos de tiempo (timestamps) a los diferentes componentes del sistema que los soliciten. Dichos sellos de tiempo contienen fecha y hora en la que se pidió el sello de tiempo, así como un resumen firmado del documento para el que se pidió.

De esta forma si un componente solicita un sello de tiempo sobre un TCE, tendrá que mandarle un resumen criptográfico del mismo a la entidad de sellado de tiempo. Dicha entidad genera un sello de tiempo añadiendo la fecha y hora actual al resumen y firmando el conjunto. Dicho sello de tiempo una vez añadido al TCE permite situarlo dentro de un marco temporal.

Si además se usa este procedimiento de sellado de tiempos en el proceso de firma electrónica de un TCE se consigue establecer de forma segura el momento exacto en que se ha firmado dicho TCE.

Entidad de Revocación online

Es la entidad encargada de ofrecer, en tiempo real, el estado de revocación de un certificado, algo muy necesario en el tipo de transacciones que estamos manejando.

Hub Transaccional

Todas las comunicaciones entre entidades se van a realizar mediante buses de mensajería.

El Hub transaccional es una aplicación informática que permite coordinar a todos los actores y procesos que intervienen en una operación con un TCE mediante el control de transacciones atómicas. Así, pues, coordina las diversas operaciones de los servicios de emisión, depósito, transmisión y cobro.

Este elemento se basa en el tratamiento de mensajes, interpretando sus atributos conduciendo las transacciones según este formato a los componentes que efectúan los tratamientos correspondientes.

La responsabilidad de ejecutar el proceso de negocio y de canalizar los mensajes a las entidades externas que se encar-

gan de su resolución se reparte entre una serie de componentes que forman parte del Hub. Estos componentes interpretan, conducen y transforman el contenido para entregarlo a las entidades distribuidas participantes (léase GTCE, fuente de verdad o entidades financieras) en el formato requerido e incluyendo toda la información necesaria para su participación.

Arquitectura global

La arquitectura global del sistema queda reflejada en la siguiente figura:

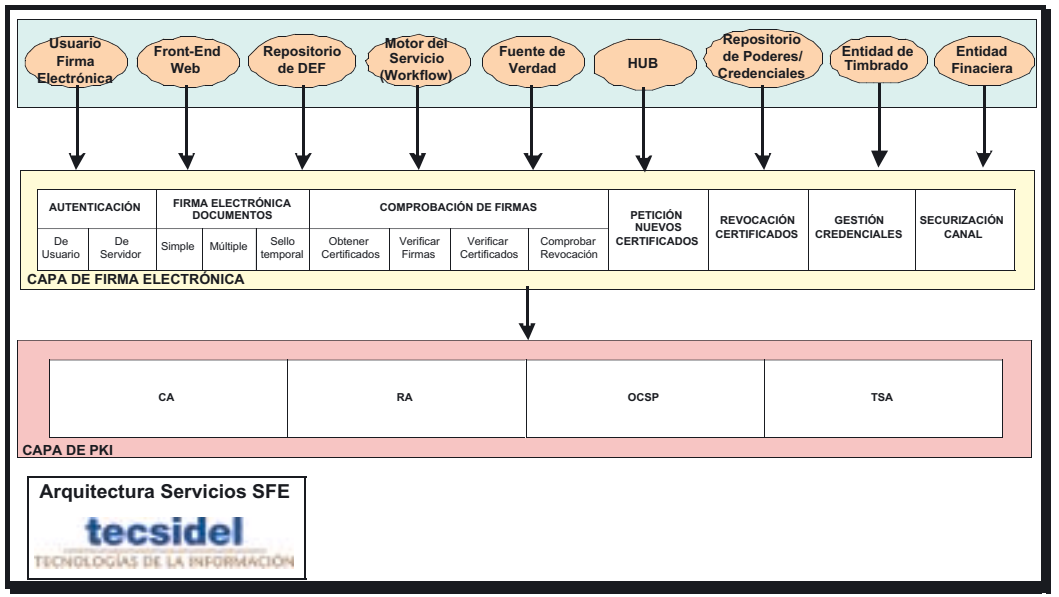

Figura: Arquitectura de Actores

2.4 Marco legal

Un entorno seguro debe basarse, no solo en el uso intensivo de la firma electrónica, sino en potenciar la firma electrónica avanzada, concepto que aúna aspectos tecnológicos y legales.

Una firma electrónica avanzada, según la Directiva Europea del 13/12/1999, cumple los siguientes requerimientos legales: Identifica al firmante de manera única y se crea usando métodos bajo el control del firmante, de manera que queda vinculada a él mismo y a los datos a los que se refiere, lo que permite detectar cualquier modificación ulterior de éstos.

En un documento firmado con una firma electrónica avanzada se combina, en la firma, tanto la integridad del contenido como la autenticidad del autor. Éstas firmas, cuando se basen en un certificado reconocido, expedido por un prestador de servicios de certificación autorizado , tienen el mismo valor jurídico que las manuscritas.

El avance del marco legal hacia los nuevos escenarios incluye las últimas directivas del Parlamento Europeo y del Consejo de la Unión Europea. Fijando, no solo los requerimientos de la firma electrónica avanzada, sino también los requerimientos de contenidos mínimos de información exigibles a los prestadores de servicios con el fin de poder salvaguardar mejor los derechos de los consumidores y usuarios de Internet.

Actualmente existen los instrumentos necesarios para un consentimiento electrónico eficaz. Aun así el rápido avance de la sociedad de la información y del comercio electrónico, que se está desarrollando muy por encima de las previsiones, causa que cualquier medida legislativa parezca estar dotada de cierta provisionalidad.

Para evitar esta sensación de lentitud del sistema jurídico en reaccionar ante la realidad social, la iniciativa propone un desarrollo multidisciplinar que aúna los esfuerzos en el marco tecnológico y jurídico con el fin de conseguir una convergencia de forma ágil.

Esta convergencia debe producirse a dos niveles:

- La Ley cambiaria y del cheque, que apoya la gestión de este tipo de documentos, debería ajustarse al nuevo escenario.
- El anteproyecto de Ley de firma electrónica debería recoger nuevas definiciones que permitieran la comprobación de la vigencia de las firmas en distintos plazos de tiempo. Requisito para procesos complejos como son los negocios jurídicos de la operativa cambiaria.

En este sentido, se propone establecer la definición de firma electrónica completa como la firma electrónica junto con sus datos de validación, que permite la validación de la misma a medio y largo plazo, es decir cuando los datos de creación de la firma del firmante hayan dejado de estar vigentes.

La razón por la que conviene diferenciar firma electrónica completa y distinguirlo de firma electrónica avanzada es que firma

electrónica avanzada no incluye necesariamente los datos de validación. Y éstos son imprescindibles en el caso de que sea necesario validar una firma después de la revocación del certificado que avala los datos de verificación de la misma.

2.5 Conclusiones

El uso de títulos cambiarios, letras, cheques o pagarés, para realizar pagos es algo común en el mundo físico. El proyecto FIRMA pretende la trascripción de los títulos a formato electrónico, y el despliegue de un entorno que permita estudiar las posibilidades, sobretodo del marco legal, y hasta que punto la tecnología está preparada. Por eso se escoge un escenario complejo como el de los títulos

Trasladar la operativa cambiaria al mundo virtual aporta una serie de ventajas:

- Procesamiento inmediato.
- Reducción de costes por desaparición del papel.
- Evitar los errores derivados del proceso manual.
- Disminución del tiempo de resolución de conflictos.
- Evitar la falsificación. (que se da especialmente en el caso de los cheques)

Adicionalmente supone un avance en el sector financiero, pues aporta al campo de los medios de pago un sistema seguro, reconocido en el marco jurídico y apoyado por instituciones públicas. Lo que permitirá rescatar unos medios de pago que por sus desventajas (coste, tiempo de proceso, etc.) han caído en desuso. Cediendo terreno a alternativas electrónicas pero basadas en acuerdos contractuales entre la entidad y el cliente.

El desarrollo de proyectos como los enmarcados dentro de la iniciativa PISTA suponen un avance en el desarrollo de la sociedad de la información al tiempo que acercan a los usuarios a las nuevas tecnologías desde un enfoque que trata de convencer de sus beneficios.

El desarrollo del proyecto FIRMA, que trae consigo el uso intensivo de la firma electrónica, debería sentar las bases para que otras iniciativas de desmaterializar la información entre proveedor y cliente puedan acogerse a los estándares de seguridad resultado de este proyecto. En esta línea encontramos ya diversas iniciativas alrededor de la facturación electrónica, impulsadas con la aprobación de recientes Directivas Europeas.