tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

359

27 DE MAYO DE 2005. PRIMER DOCUMENTO ELECTRÓNICO FIRMADO POR UNA ADMINISTRACIÓN PÚBLICA CON TERCEROS

Fernando Gil Vázquez
Técnico del Servicio de Desarrollo de la Sociedad de la Información
Consellería de Innovación e Industria, Xunta de Galicia

Pablo Valdés Álvarez
Técnico del Servicio de Informática
Consellería de Innovación e Industria, Xunta de Galicia

Josefina Fernández Álvarez
Gerente de Proyectos
Altia Consultores, S.L.

Benito Carballo Santaclara
Jefe de Proyectos
Altia Consultores, S.L.

Fernando Gil Vázquez
Pablo Valdés Álvarez
Josefina Fernández Álvarez
Benito Carballo Santaclara

Palabras clave

Documento electrónico, firma electrónica, dispositivo de verificación de firma, portafirmas digital, seguridad jurídica.

Resumen de su Comunicación

El 27 de mayo de 2005 se firmó en Santiago de Compostela un documento electrónico entre la Xunta de Galicia y 3 operadoras de telecomunicaciones, no existiendo constancia documental de que tras año y medio de publicarse la Ley 59/2003, de 19 de diciembre, de firma electrónica, alguna Administración Pública en España hubiese realizado un documento de este tipo.

En esta comunicación se expone la necesidad de emplear aplicaciones que sirvan de Portafirmas Digitales, con las debidas garantías, y del alcance de los dispositivos de verificación de firma electrónica.

Se exponen los problemas detectados en esta experiencia y la conveniencia de disponer de medios públicos independientes que permitan verificar los documentos electrónicos firmados y den garantía jurídica a la realización de este tipo de actos entre partes, conforme a la Ley 59/2003.

Fernando Gil Vázquez
Pablo Valdés Álvarez
Josefina Fernández Álvarez
Benito Carballo Santaclara

27 DE MAYO DE 2005. PRIMER DOCUMENTO ELECTRÓNICO FIRMADO POR UNA ADMINISTRACIÓN PÚBLICA CON TERCEROS

1. Idea inicial

Ante el lanzamiento el 27 de mayo de 2005 de una iniciativa de la Xunta de Galicia en materia de Sociedad de la Información, que apostaba por el empleo de la firma electrónica en las empresas, se valoró la conveniencia de que el propio convenio que recogía esta iniciativa también fuese suscrito empleando la firma electrónica de los participes en el mismo.

Desde la Xunta de Galicia contábamos con la experiencia de la gestión de nuestro propio Registro Telemático, con lo cual se disponía de conocimientos de primera mano. No es nada nuevo que en esta Administración, como en otras, se generan a diario apuntes en estos registros telemáticos con firma electrónica de documentos. Además cualquier persona iniciada en el tema sabe que no existe ningún problema o dificultad técnica entre realizar una firma electrónica o varias sucesivas, por lo que la firma de un documento con múltiples firmantes no parecía entrañar complejidad añadida.

Con estas premisas iniciales nos planteamos las vías a seguir para darle forma y validez a ese acto de firma, dado que no queríamos realizar una entrada firmada en un registro telemático, sino que buscábamos generar un documento electrónico estrictamente respetuoso con la Ley 59/2003, de 19 de diciembre, de Firma Electrónica (en adelante LFE), y que además dicho documento electrónico pudiera ser verificado por un tercero, conforme a la propia LFE, sin necesidad de intervención de la Administración actuante.

Buscando mejorar la información de la que disponíamos empezaron a surgir las primeras dudas al no encontrar ningún antecedente documentado, ¿pero esto, por qué no lo ha hecho nadie antes?, ¿qué dificultades reales entraña? Porque es bien cierto que en el mercado se encuentran distintas aplicaciones de firma de documentos y de verificación, pero no encontrábamos una aplicación que nos resultase plenamente satisfactoria desde el punto de vista técnico y legal.

2. Análisis del problema y creación de un portafirmas digital.

Del análisis del problema se llego al convencimiento que no era posible realizar un acto de firma con las debidas garantías si no se procedía a desarrollar una aplicación informática específica, un Portafirmas Digital, que permitiese ejecutar todo el proceso conforme a la LFE y que generase un documento electrónico que fuese verificado por la propia aplicación informática.

El Portafirmas Digital tenía que disponer de las siguientes funcionalidades:

2.1. Comprobación de la validez de los certificados personales de los firmantes contra la Autoridad de Registro que los había expedido.

En este caso los certificados a emplear eran los clase 2 CA de la FNMT, por lo que se realizó la comprobación individual de cada certificado como paso previo a iniciarse el acto de firma contra el propio servicio web de la FNMT.

La Xunta de Galicia, como muchas otras administraciones, tiene un convenio con la FNMT que le permiten verificar “en línea” el certificado digital de un ciudadano antes de permitir acceso a sus aplicaciones administrativas, pero no se optó por esta vía de comprobación, entendiendo que debía emplearse una

opción más general y disponible por cualquier usuario.

2.2. Empleo de una aplicación de firma, para firmar el documento.

Era necesario disponer de una aplicación que seleccionase un archivo inicial sin firmar, y procediese a elaborar un documento electrónico formado por el archivo inicial y otro archivo en el que se recogen las características específicas de la firma de dicho archivo inicial.

2.3. Permitir la firma secuencial de los distintos firmantes.

También se tenía que permitir la firma secuencial de distintos firmantes modificando las características del archivo de firmas, de forma que se genera un único archivo de firmas con todos los firmantes, y no múltiples firmas individuales de un mismo archivo.

Era también de la mayor importancia que el proceso de firma secuencial no fuese destructiva de las firmas anteriores si existía algún error durante el proceso, tal como equivocación en el PIN o interrupción del proceso. De modo que fuese posible reiniciar la aplicación salvaguardando lo ya firmado.

2.4. Creación de un dispositivo de verificación de firma conforme a la LFE.

Además se adoptó la decisión de que el dispositivo de verificación tenía que entregar un mensaje lo suficientemente contundente y explícito sobre la legalidad del documento electrónico. No nos conformábamos con una simple pantalla de verificación, que a nadie contenta. A falta de otros referentes documentados, tuvimos que definir ese texto. Pero además, consideramos de la mayor importancia que la aplicación facilitase la información de verificación suficiente para que cualquiera pueda realizar con sus medios técnicos una verificación sin necesidad de disponer de dicha aplicación. Se adjunta el resultado de este dispositivo de verificación de firma como Anexo 1 a esta comunicación.

Fernando Gil Vázquez
Pablo Valdés Álvarez
Josefina Fernández Álvarez
Benito Carballo Santaclara

Figura 1. Pantalla de inicio del Portafirmas Digital para la firma del convenio de 27 de mayo de 2005.

3. El propio acto de firma

Se organizó el acto contando con la firme decisión, pese a los posibles condicionantes técnicos, de efectuar un acto abierto y ante la prensa, con proyección de todas las pantallas de la aplicación con los pasos realizados por los firmantes.

La voluntad por impulsar el uso de la firma electrónica hizo que se reuniesen en la misma sala los representantes de la Xunta de Galicia, de Comunitel Global, de R Cable y Telecomunicaciones Galicia y de Telefónica de España, para plasmar su firma electrónica mediante PIN, en lugar de hacerlo con pluma.

El hardware elegido fue un ordenador portátil, con la aplicación instalada en local, pero con acceso a internet para verificar los certificados contra la web pública de la FNMT. Este equipo disponía de controladores para la lectura de tarjetas criptográficas de la FNMT, así como de los "tokens" USB ikey3000 de Rainbow Technologies ®, habiéndose remitido con anterioridad sendos dispositivos para almacenar certificados a cada firmante.

Se hizo necesario realizar una inserción secuencial de los dispositivos de cada firmante, dado que el software de gestión de dispositivos criptográficos empleado en ese momento no permitía gestionar varios dispositivos con almacén de certificado conectados a la vez al mismo PC. Desde su asiento cada firmante pudo introducir el PIN de su certificado gracias a un teclado inalámbrico enlazado al portátil, viendo todo el proceso proyectado en la pantalla.

Uno de los firmantes olvidó el PIN de su tarjeta FNMT por lo que poco faltó para que no pudiese participar en el acto, por fortuna recordaba el PIN del otro dispositivo y llevaba encima el "token" USB, por lo que finalmente pudo firmar sin ningún problema.

Figura 2. Carátula del CD-Rom con el documento electrónico

Finalizado el acto, cada asistente pudo llevarse un ejemplar en CD-Rom del documento electrónico original firmado, con su dispositivo de verificación.

4. Documento electrónico, ¿nuevo problema?

Después de realizado el acto firma electrónica, ahora viene el siguiente paso ¿quién se cree que ahí hay un documento con plena validez legal? En estos temas no basta con tener fe, sino que es necesario habilitar los cauces que garanticen seguridad jurídica. En esta línea se trabajó en la realización del dispositivo de verificación de firma con los resultados que se adjuntan en el Anexo 1.

Entendemos que un dispositivo de verificación de firma puede cumplir la LFE, como entendemos que es este caso, pero detectamos la necesidad de que ese documento firmado lo pueda llevar un tercero ante

cualquiera y pueda acreditar su validez, porque la fe en la tecnología no está al alcance de todos, ni tan siquiera de los jueces.

El escepticismo o la sensación de inseguridad sobre este tipo de documentos no van a desaparecer de la noche a la mañana, pero se deben afrontar medidas públicas que minimicen este posible rechazo ante lo poco conocido.

Baste decir que todos los convenios que firma la Xunta de Galicia se archivan centralizados en un órgano central, y cabe imaginar que la cara del archivero, cuando abrió un típico sobre esperando un montón de papeles y le llega un CD-Rom con un documento original, debió de ser para grabar.

5. Lo que se nos viene encima.

Esta experiencia ha servido para centrar buena parte de los problemas inherentes a la aplicación real de la LFE, en la realización de documentos electrónicos, entre ellos:

- La necesidad de realizar configuraciones previas de recursos y opciones de seguridad en los equipos en los que se pretende ejecutar aplicaciones de firma. La Xunta de Galicia ha desarrollado un "asistente" automático de configuración con muy buenos resultados, pero en algún caso sigue necesitándose configuración "manual" en las propiedades de uso de los certificados o para salvar restricciones del navegador empleado.

- Se echa en falta un entorno unificado de acceso criptográfico que sea independiente del navegador y del sistema operativo. En este caso y por premura en los plazos, se empleó la máquina virtual de Microsoft para el applet de firma porque facilitaba la integración con la librería Capicom sin necesidad de otras librerías adicionales. Versiones posteriores del applet de firma de la Xunta de Galicia abandonan la máquina de Microsoft y usan ya la máquina java de Sun (en realidad se soporta cualquier máquina java compatible con la versión 1.4 o superior) con acceso directo a la CryptoAPI de Windows.

- Resulta bastante evidente el esfuerzo al que se enfrenta individualmente cada Administración ante el hecho de no disponer de software con garantía institucional que sirva de "applet" de firma multicertificado. Además este proceso está sujeto a mejora continua, dado que si se quiere extender la funcionalidad, es necesario hacer desarrollos para acceder a los certificados desde otros sistemas operativos o usando los módulos que se integran en los navegadores a los distintos dispositivos criptográficos.

- La inexistencia de aplicaciones públicas que permitan al ciudadano en general la verificación de documentos electrónicos firmados por un único firmante o por varios y con independencia de los distintos formatos de codificación de la firma electrónica que se hayan empleado (PKCS#7, CMS, ETSI TS 101 903,...)

Pese a estas dificultades, y tal como ya se han ido imponiendo el uso de certificados digitales en ámbitos tributarios, estas prácticas pueden cambiar la necesidad de mucha "presencia física" ante las Administraciones, evitando viajes y reuniones. Basta con realizar un portafirmas digital accesible en web para que cualquier empresa o ciudadano firme sus contratos con la administración de turno, pero hay que poner los medios para que los documentos electrónicos generados sean totalmente verificables por un tercero, sin necesidad de que intervenga ninguna de las partes.

Dicho esto debemos insistir en la necesidad de disponer de recursos públicos gratuitos de verificación de documentos electrónicos, si es que se pretende que su uso salte de la mera marginalidad, siendo de utilidad tanto en lo que pudiera interesar a las Administraciones Públicas como a las relaciones privadas entre ciudadanos y empresas.

También se hecha en falta avanzar sobre las características técnicas mínimas que deben de tener los documentos electrónicos para que se puedan guardar con seguridad y sean verificables con posterioridad con independencia de los estándares y aplicaciones informáticas actuales.

Tras el mismo acto de firma electrónica del convenio y en un momento de lucidez por lo que habíamos hecho, uno de los firmantes sugirió: ¿y ahora por qué las administraciones no firman electrónicamente todos sus pliegos de contratación cuando se publiquen, de modo que se garantice que éstos no se modifican? Y ¿cómo se garantiza o se comprueba este asunto si no existen mecanismos independientes de verificación y con suficiente autoridad?. Esto vale también para cualquier información pública que merezca la pena garantizar su integridad, como dar validez legal a los archivos electrónicos de los Diarios Oficiales, notas de prensa, partes meteorológicos, etc. A ver quien se anima y da el primer paso.

Agradecimientos:

La realización del documento electrónico aquí descrito no hubiera sido posible sin la colaboración de todo el equipo humano responsable del Registro Telemático de la Xunta de Galicia, adscrito a la Consellería de Presidencia, Administracións Públicas e Xustiza.

Fernando Gil Vázquez
Pablo Valdés Álvarez
Josefina Fernández Álvarez
Benito Carballo Santaclara

Anexo 1. Resultado del dispositivo de verificación de firma

Alcance de la verificación sobre documento electrónico.

Los términos incluidos en este texto en cursiva se corresponden con definiciones literales conforme a lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

1. Generación del documento electrónico.

Esta aplicación informática está desarrollada para generar un documento electrónico, conforme a la Ley 59/2003, de 19 de diciembre, de firma electrónica partiendo de un documento inicial sin firmar: "D:\convenio_verificacion\convenio\convenio.pdf".
Los firmantes de dicho documento inicial, realizan con la ayuda de esta aplicación informática la firma electrónica reconocida, con sus respectivos certificados electrónicos reconocidos. Estas firmas electrónicas quedan recogidas en el fichero informático "D:\convenio_verificacion\convenio\convenio.pdf.pk7".
El documento electrónico generado está formado por ambos ficheros informáticos, el inicial y el de firmas:

- D:\convenio_verificacion\convenio\convenio.pdf
- D:\convenio_verificacion\convenio\convenio.pdf.pk7

2. Verificación del documento electrónico.

Esta aplicación informática dispone de un dispositivo de verificación de firma, conforme a la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el que se obtuvo el siguiente resultado:
El documento inicial "D:\convenio_verificacion\convenio\convenio.pdf" se verificó correctamente con el software criptográfico CAPICOM de Microsoft, contra el fichero de firmas "D:\convenio_verificacion\convenio\convenio.pdf.pk7" en formato PKCS#7.
La verificación del documento se realizó empleando la función correspondiente proporcionada por la librería CAPICOM de Microsoft, transformando previamente el fichero del documento en un objeto de tipo "String Unicode".
El documento inicial no fue modificado tras la firma y fue firmado por:

- DELGADO ARCE JOSE ANTONIO con NIF 12345678Z con certificado de la FNMT clase 2CA válido desde 9/5/2005 hasta 9/5/2008.
- RODRIGUEZ YUSTE JUAN con NIF 12345678Z con certificado de la FNMT clase 2CA válido desde 11/5/2005 hasta 11/5/2008.
- DOPICO PEREZ ARTURO con NIF 12345678Z con certificado de la FNMT clase 2CA válido desde 13/5/2005 hasta 13/5/2008.
- VEIGA ABELEDO JOSE ANGEL con NIF 12345678Z con certificado de la FNMT clase 2CA válido desde 16/5/2005 hasta 16/5/2008.

Fecha de la verificación: 9/3/2006 18:48 (según el reloj local del equipo empleado para realizar la verificación)

La verificación del documento podría realizarse también con cualquier otro software de verificación, teniendo en cuenta que previamente habría que transformar el documento inicial "D:\convenio_verificacion\convenio\convenio.pdf" (cadena de bytes) a una cadena de caracteres Unicode.

Fernando Gil Vázquez
Pablo Valdés Álvarez
Josefina Fernández Álvarez
Benito Carballo Santaclara

Nota a este Anexo: en este documento, reproducido para Tecnimap2006, se han eliminado los NIF de los firmantes, sustituyéndolos por 12345678Z