FIRMA ELECTRÓNICA DEL FUNCIONARIO EN EL PROCEDIMIENTO ADMINISTRATIVO. PROPUESTA DE CERTIFICADO DE ATRIBUTOS Y NUEVO SISTEMA ADICIONAL DE ACTIVACIÓN.

Rafael Ferrando Martínez
María José Portero López

Universidad de Murcia

Resumen.

En el artículo 3.4 de la Ley 59/2003 de 19 diciembre, de Firma Electrónica (LFE), se establece que la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los datos consignados en papel.

El modo de activación de la e-firma carece de la característica fundamental de la grafía biológica, en la que se pone de manifiesto tanto la anatomía como el funcionamiento de un determinado gesto, lo que le da un carácter personalizador. Una persona puede encontrarse en condiciones de firmar electrónicamente un documento siempre que conozca la clave de activación y tenga acceso a los medios para crearla.

Para corregir esta posibilidad de uso de la e-firma por persona distinta del titular, se propone un mecanismo adicional que habilite el sistema de autenticación del proceso de la firma, consistente en la captura de la firma manuscrita en una tarjeta digitalizadora y su identificación y verificación, mediante un análisis biométrico de la firma.

El diseño de una plataforma de e-firma en una administración debe ser un objetivo de la propia organización, siendo esta una cuestión de estrategia fundamental en la implantación de la e-admón.

En base al artículo 19 de la LAECSP que manifiesta que la identificación y autenticación del ejercicio de la competencia de la Administración Pública**,** cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio, se propone el desarrollo de un sistema de e-firma de atributos, que identifique de forma conjunta al titular del puesto de trabajo y a la Administración en la que presta sus servicios, activada con la captura y validación de un criptosistema biométrico.

La implementación de este proceso de e-firma, tiene que contemplar que un documento puede requerir mas de una firma (cofirma), incluyendo la secuencia de ellas, así como la posibilidad de firmar lote de documentos.

Introducción.

El día 23 de junio de 2007, se publicó en el Boletín Oficial del Estado, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), entrando en vigor el día 24 de junio. A partir de este momento la Administración queda obligada a transformarse en una administración electrónica al servicio del ciudadano, regida por el principio de eficacia que proclama el artículo 103 de nuestra Constitución.

De ello se percató la Ley 30/1992 de 26 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PAC), que en su primera versión recogió ya en su artículo 45 el impulso al empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos por parte de la Administración, al objeto de desarrollar su actividad y el ejercicio de sus competencias y de permitir a los ciudadanos relacionarse

con las Administraciones cuando fuese compatible con los «medios técnicos de que dispongan».

En el momento actual, el documento es el elemento más característico de nuestra civilización. Nos encontramos inmersos en una sociedad enormemente burocratizada, en la que todas las gestiones y las relaciones entre las personas se realizan a través del documentos [ANT, 2005].

La LAECSP regula la validez de los documentos y sus copias y la forma de que el documento electrónico opere con plena validez y, en su caso, la forma en que los documentos convencionales se transformen en documentos electrónicos. Otra cuestión que se aborda en esta Ley es regular las formas de identificación y autenticación, tanto de los ciudadanos como de los órganos administrativos en el ejercicio de sus competencias, utilizando los sistemas establecidos de firma electrónica.

El artículo 19 de la LAECSP manifiesta que la identificación y autenticación del ejercicio de la competencia de la Administración Pública, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio.

De acuerdo con el apartado segundo de este artículo, y con la necesidad de incorporar las nuevas tecnologías al funcionamiento interno de las AA-.PP, el objetivo es desarrollar la implantación de un proceso para proveer al funcionario de un sistema de firma electrónica que identifique de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. Se trata de acompañar a la e-firma realizada por un funcionario en un documento administrativo electrónico, de un certificado de atributos, de tal manera que el acto será válido una vez que el sistema realice la comprobación que el funcionario tiene atribuida la competencia para realizarlo.

Este desarrollo debe tener en cuenta que, aunque los documentos administrativos normalmente están firmados por una sola persona, bien sea al ejercer una competencia por el cargo que desempeña, o por su condición de secretario de un órgano colegiado, por el que da fe de los acuerdos de este, también existen documentos que requieren más de una firma, como es el caso de la disponibilidad de fondos de las cuentas financieras de las que las administraciones son titulares. Para atender esta situación el sistema de firma electrónica (e-firma), deberá contemplar la posibilidad de multifirma en un documento, cuales son estos documentos y los firmantes, así como el orden secuencial; de tal manera que el segundo y sucesivos firmantes puedan comprobar que las anteriores se han realizado.

Los flujos de trabajo administrativos, basan su funcionamiento en la definición realizada sobre el proceso. Automatizan el conjunto de expedientes de la organización, proporcionando un seguimiento eficiente y fiable durante el tiempo que dure su ejecución, pudiendo abarcar más de un área de la organización [ULT, 1998]. Cada usuario del sistema de gestión debe disponer de una bandeja de procesos pendientes de su actuación, permitiendo, entre otras funciones, la e-firma de documentos por lotes.

Estos desarrollos están orientados a unificar sistemas y ahorro de costes, alcanzando un mayor énfasis en las Comunidades Autónomas que deben tutelar a otras de menor capacidad de innovación, como es el caso de las Entidades que integran la Administración Local de pequeña capacidad presupuestaria; facilitando que puedan ofrecer los derechos reconocidos en el artículo 6 de la LAECSP, a partir del 31 diciembre de 2009. En este sentido se manifiesta el artículo 45 de la LAECSP al establecer que las Administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios o cuyo desarrollo haya sido objeto de contratación, podrán ponerlas a disposición de cualquier Administración sin contraprestación y sin necesidad de convenio.

Situación actual.

La firma electrónica.

La escritura constituye una grafía biológica en la que se pone de manifiesto tanto la anatomía como el funcionalismo de un determinado sujeto, por lo que posee carácter personalizador. Escribir es, ante todo, la ejecución de un gesto y cualquier gesto, por peculiar que sea, sólo es el resultado de la puesta en marcha de determinadas regiones cerebrales en las cuales se conciben y controlan los movimientos. Escribir es en definitiva, una ejecución individual, la materialización singular de la personalidad que sin duda pone de manifiesto los aspectos más íntimos del psiquismo humano. [ANT, 2005].

La voluntad de una persona queda acreditada en todos los casos en que la firma representa un consentimiento y un conocimiento del contenido, no se puede firmar de forma automática. Por ello esta firma debe realizarse con un certificado personal y llevar asociado un fechado de tiempo. Igualmente, una persona puede firmar un documento en función de sus distintas actuaciones (personal, en calidad de su cargo, representación, etc). Actualmente la calidad la proporciona el contexto del documento y el pie de firma sin que la firma personal sea distinta. En el mundo telemático hay dos alternativas: puede hacerse igualmente en función del contexto o mediante un certificado con atributo. La alternativa de un certificado con atributo es más segura.

La identidad digital o electrónica es el conjunto de datos, independientemente del soporte, que permiten a través de medios telemáticos asegurar la identidad de una persona. La firma electrónica confiere al documento determinadas características como integridad y no repudio, pero la firma no tiene el mismo significado en todo los casos.

Así como hay que diferenciar la identidad y firma, aunque están basados en los mismos elementos técnicos, se debe diferenciar la identidad y la acreditación de voluntad. El DNIe proporciona dos certificados diferentes para estas dos funciones.

El uso de la criptografía, en la que se basa la e-firma, posee otras utilidades a través de la e-firma, saber a qué hora exacta y en qué fecha se firmó un documento, detectar posibles intentos de modificación del mismo o no autorizados, o poner en clave información confidencial.

En la actividad administrativa, no todos los procesos tienen la misma relevancia jurídica (actos de trámite, actos que ponen fin a la vía administrativa, etc.), en base a lo cual hay que identificar que tipos de e-firma se pueden-deben emplear en cada uno. Así podemos emplear la firma electrónica (conjunto de datos recogidos en forma electrónica, que formalmente identifican al autor), en la mayoría de los actos de trámite. La e-firma avanzada, que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. Estos dos sistemas de e-firma, podrán ser utilizados en los diferentes procedimientos administrativos. Por último la e-firma reconocida es la e-firma avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma, teniendo el mismo valor a efectos legales que la firma manuscrita. El DNIe podrá ser utilizado por las personas físicas, en todo caso y con carácter universal.

En el artículo 19 de la LAECSP se dice que la identificación y autenticación del ejercicio de la competencia, cuando se utilicen medios electrónicos, se realizará mediante e-firma del personal a su servicio. Dice se “realizará” no “se podrá realizar”, por lo que está obligando a que la actividad de la Administración, cuando se utilicen medios electrónicos, necesariamente se tendrá que firmar electrónicamente.

Para la actuación administrativa automatizada, contemplada en el artículo 18 de la LAECSP, la Administración Pública deberá identificar y autenticar, determinando los supuestos de utilización los siguientes sistemas de e-firma:

- Sello electrónico de Administración Pública, mediante el certificado electrónico. (Sellado electrónico de órganos administrativos que identificará al órgano administrativo o al puesto directivo que tenga atribuida la competencia y a la persona física titular del órgano o puesto).

- Código seguro de verificación vinculado a la Administración Pública y en su caso a la persona firmante, permitiéndose en todo caso la comprobación de la integridad del documento.

Tarjeta de identidad.

El artículo 19.2 de la LAECSP dispone que cada Administración Pública podrá proveer a su personal de sistemas de e-firma, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que prestan sus servicios.

Actualmente hay un buen número de Administraciones que tienen distribuido un documento de identidad para su personal, que contiene la posibilidad de alojar un certificado de e-firma similar al del DNIe. Con la entrada en vigor de la LAECSP (artículo 19), la firma electrónica basada en el Documento Nacional de Identidad, del personal al servicio de las Administraciones Públicas, podrá utilizarse para la firma cuando se utilicen medios electrónicos, estas Administraciones deben reconfigurar estos sistemas de identificación de

manera que se de preferencia al nuevo DNIe, no solamente para el uso de la firma electrónica sino para los procesos de identificación. En definitiva el DNIe está encaminado a sustituir todos los soportes de identificación (hay en marcha algunos desarrollos de utilidad, por el que este documento sustituye a las tarjetas de crédito y débito).

Actualmente, pese a que la expedición del nuevo DNIe en la Región de Murcia está prevista para el 2008, la Universidad de Murcia ya ha adaptado la aplicación de los sistemas de procedimientos administrativos, como es el caso de la firma de actas de calificaciones de exámenes, permitiendo la e-firma con la tarjeta identificativa que esta Universidad tiene expedida para su personal (con certificado de la FNMT), así como con DNIe.

Sellado de tiempo.

En el artículo 29.2 de la LAECSP, se establece que los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos. Este sellado de tiempo se acreditará a cargo de un tercero de confianza, incluyendo la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Este sellado, del que la LAECSP dice que será de aplicación a los documentos cuya naturaleza así lo requiera, deja indefinido que tipo de documentos o cuales son las características que deben cumplir aquellos a los que hay que aplicarles este proceso. Ello obliga a que las Administraciones deberán identificar en sus procedimientos automatizados, a que documentos hay que aplicárselo.

No obstante, una gran parte de los documentos que las AA.PP elaboran se crean en soportes electrónicos, apoyados en la información que reside en las bases de datos que gestionan. Estos sistemas registran una auditoría, en la que se almacena la información de quien, que día y a que hora, ha realizado cada registro, modificado o borrado. Por ello, aunque de forma indirecta, los sistemas modernos de gestión documental, almacenan la información correspondiente al sellado de tiempo. Otra cosa distinta es incluir estos datos en el propio documento.

Otra problemática que se presenta con el sellado de tiempo es la correspondencia entre la fecha real de la firma y el fechado del documento. ¿hay alguien que no halla firmado un documento fechado en día distinto al que realmente se plasma la rúbrica?, ¿cuántos documentos no electrónicos se fecha con la hora?. A modo de ejemplo podemos citar la cantidad de documentos que se firman con fecha último día hábil del año natural, en los procesos de cierre de un ejercicio económico.

Firma de atributos.

En el artículo 19 de la LAECSP se contempla que la firma electrónica del personal al servicio de las AA.PP podrá identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración, así como la competencia del funcionario firmante para realizar el acto administrativo. Si partimos de la

base de que el documento se firma con el certificado personal de la persona, esta firma no es suficiente para que el acto adquiera validez, es necesario que esté realizado por un funcionario que tenga la competencia vigente para realizarlo. Pongamos como ejemplo la firma electrónica de un proyecto de obra por un arquitecto, la sola firma no acredita que esa persona tenga la competencia habilitada para la firma de ese documento, por lo que tendrá que ir acompañada por la acreditación (certificado de atributos) de una entidad que avale que esa persona en el momento de hacer uso de su e-firma, disponía de la competencia para realizar la firma de ese documento.

Las AA.PP. deben proporcionar al personal a su servicio certificados de e-firma que identifiquen a la persona, el puesto que ocupa y el órgano o entidad en el que lo desempeña; siempre que las funciones que desarrollan precisen del uso de tales certificados.

Biometría de la firma.

La biometría es un sistema automatizado de reconocimiento humano a través de sus características fisiológicas (huellas dactilares, iris, rostro, retina,…) o de comportamiento (voz, firma,…).,

Los métodos tradicionales de autenticación por contraseña o tarjetas inteligentes trabajan en base a lo que se conoce o posee. y pueden ser perdidas, sustraídas y/o duplicadas. Cosas que una persona conoce, tales como passwords y códigos, pueden ser olvidados, sustraídos y/o duplicados. En lugar de ello**,** los sistemas biométricos se fijan en "quién" es la persona, basándose en una única e inalterable característica humana que no puede ser perdida, olvidada, sustraída o duplicada. La biometría, por lo tanto, proporciona el máximo nivel de seguridad, conveniencia y facilidad de usar.

El reconocimiento biométrico puede ser del tipo Identificación o Verificación. En el primer caso se trata de saber quién es la persona, es decir ubicarla dentro de un conjunto de usuarios; en el segundo, en cambio se busca verificar que un usuario sea realmente quien dice que es.

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documento o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma. En los modelos biométricos se utiliza además la forma de firmar, las características dinámicas (por eso se les suele denominar Dynamic Signatura Verification, DSV): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con el que se realiza cada trazo.

El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: captura o lectura de los datos que el usuario a validar presenta, extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar), comparación de tales

características con las guardadas en una base de datos, y decisión de si el usuario es válido o no.

Las soluciones biométricas no almacenan la propia información capturada sino una representación simbólica en base a modelos matemáticos, con los cual se gana en exactitud y privacidad.

En un futuro no muy lejano estos serán los sistemas que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario: son más amigables para el usuario (no va a necesitar recordar password o números de identificación complejos, y, como se suele decir, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará de su mano o su ojo) y son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética.

Propuesta de implantación de un sistema de firma electrónica para los procedimientos internos (back office) en una Administración Española.

Cualquier sistema de e-firma, tendrá que ajustarse a lo dispuesto en el artículo 25 de la LFE, en el que se establecen los dispositivos de verificación de firma electrónica. Hay que tener en cuenta que los datos de verificación de firma son los códigos o claves criptográficas públicas, que se utilizan para verificarla. Los dispositivos de verificación de e-firma son programas o sistemas informáticos que sirven para aplicar los datos de verificación, garantizando, siempre que sea técnicamente posible, que el proceso de comprobación de una firma electrónica satisfaga, la identificación de la persona que verifica la firma; que esta se verifique de forma fiable y el resultado se presente correctamente; que la persona que verifica la e-firma pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados; que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación; que se verifiquen de forma fiable la autenticidad y la validez de certificado electrónico correspondiente; y que pueda detectarse cualquier cambio relativo a su seguridad. Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la e-firma o por terceros de confianza.

Hay opiniones que manifiestan que al no garantizarse totalmente y en todo momento el control de activación de una firma electrónica por el titular (cualquier persona que disponga del dispositivo en el que reside la firma y conozca la clave de activación, puede teóricamente usarla), mas que de firma electrónica debería hablarse de sello electrónico. Esta teoría tiene su origen en los sistemas antiguos en los que los documentos que contenían el sello oficial tenían la validez legal de documento original.

Para deshacer este argumento es por lo que se propone un modelo de firma electrónica enriquecida, que realiza la propia Administración (firma de atributos), activada con la captura y validación de un criptosistema biométrico.

Se propone la creación de un criptosistema biométrico basado en *fuzzy vault* utilizando parámetros locales de la firma manuscrita *on-line*, conforme al modelo presentado por Manuel Ricardo Freire Santos, de la Universidad Antonio Nebrija.

Los resultados que se observan en este modelo son la obtención de una tasa de falso rechazo (*False Rejection Rate,* FRR) alta, que mantiene una tasa de falsa aceptación (*False Acceptace Rate,* FAR) para falsificadores entrenados de 1,2% y para casuales de 0,3%. Esto significa que aunque el sistema no está depurado para evitar los FRR, garantiza casi totalmente que no se admitirán como válidas firmas falsas. En cualquier caso cuanto más uso de la firma se realiza en el sistema, mejores resultados ofrece, ya que se dispone de mayor número de firmas válidas de comprobación.

El modelo que aquí se propone contempla las tres grandes modalidades de identificación: para poder firmar electrónicamente un documento necesitamos conocer la contraseña que activa la firma (algo que el individuo sabe), a su vez necesitamos tener conectado el dispositivo que contiene el certificado de firma (DNIe o tarjeta de identificación con microchip que contiene la firma) que es la llave que abre el proceso de e-firma; por último necesitamos hacer uso de algo que el firmante posee: su firma manuscrita (que se realizará a través de una tarjeta digitalizadora).

El flujo de ejecución en la aplicación sería la siguiente: inicialmente el programa invoca el inicio de la operación, seguidamente se obtiene la identificación del usuario, para proceder a continuación a obtener su firma, enviando ambos datos (ID+firma) al servidor. El servidor comprueba que la identificación del usuario está autorizada para realizar el proceso de firma de atributos, si existe en la base de datos, compara el algoritmo obtenido en la firma con el que reside en la base de datos, si es exitosa (verificación), el servidor autoriza la firma, en caso contrario envía un mensaje de error al cliente, ofreciendo una segunda opción.

Debido a que la legislación actual equipara la firma electrónica reconocida a la manuscrita, la certificación de atributos de la firma y documento sólo quedará ligada al procedimiento de verificación del criptosistema biométrico.

En este trabajo se propone un sistema de firma de atributos, complementario al establecido en las normas de firma y administración electrónica.

Para la actuación del subsistema de firma de atributos, previamente hay que comprobar la autenticación e-firma, ya que las Entidades Certificadoras que expiden los certificados electrónicos efectúan una tutela y gestión permanente de los certificados electrónicos que expiden.

Bibliografía.

[ULT, 1998] ULTIMUS: *Groupware, workflow and the role of Ultimus* [en línea], Carolina del Norte: Ultimus, c1996, 15 de mayo de 1998, <http:www.ultimus.com/ultwhite/wp_group.pdf>[consultado:25 noviembre 1999].

[ANT, 2005] ANTÓN, F y otros. "Análisis de textos manuscritos, firmas y alteraciones documentales", *Tirant lo Blanch 2005* Valencia.

Abreviaturas:

e_Admón.: Administración electrónica.

e-firma: Firma electrónica.

LAECSP: Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

LFE: Ley 59/2003 de 19 de diciembre, de firma electrónica.

DNIe: Documento Nacional de Identidad electrónico.

FNMT: Fábrica Nacional de Moneda y Timbre.

AA.PP: Administraciones Públicas.

LFE: Ley 59/2003 de 19 de diciembre, de firma electrónica.