ANÁLISIS DE RIESGOS Y ADMISIÓN DEL USO DE LOS MECANISMOS DE ACREDITACIÓN DE IDENTIDAD Y VOLUNTAD: LA EXPERIENCIA DE CATALUÑA, A LA LUZ DE LA LEY 11/2007

Ignacio Alamillo Domingo
Director de asesoría e investigación
Agència Catalana de Certificació

Xavier Urios Aparisi
Director de la Asesoría Jurídica
Departament de Governació de la Generalitat de Catalunya

Palabras clave

Análisis de riesgos, contraseña, firma electrónica, evidencias electrónicas, certificación electrónica, admisión de sistemas de la firma electrónica, clasificación de evidencias electrónicas.

Resumen de su Comunicación

La Ley 11/2007 establece la posibilidad del empleo de diversos mecanismos de acreditación (identificación y autenticación) de los ciudadanos y de los órganos administrativos en la comunicación electrónica, cuyo uso debe concretarse en la normativa aplicable a cada procedimiento de acuerdo con criterios de seguridad y proporcionalidad.

Ante esta nueva regulación, esta comunicación presenta la experiencia de los últimos cuatro años en Cataluña en relación a la gestión de diversos sistemas de acreditación de la identidad y la voluntad y, en particular, con respecto a la firma electrónica, dentro de un esquema de múltiples niveles de evidencia electrónica. En definitiva, se ha buscado la admisión simplificada de los mismos y la generalización de su uso por las Administraciones Públicas Catalanas.

El análisis de riesgos y el uso de los mecanismos de acreditación de la identidad y firma electrónica en la Ley 11/2007

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (en adelante, "LAECSP") establece la posibilidad del empleo de diversos mecanismos de acreditación (identificación y autenticación) de los ciudadanos y de los órganos administrativos en la comunicación electrónica, cuyo uso debe concretarse en la normativa aplicable a cada procedimiento de acuerdo con criterios de seguridad y proporcionalidad.

El artículo 3 de la LAECSP señala, en su número 3, que una de las finalidades de la Ley es "crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos".

Por su parte, en el artículo 4 del propio texto legal se establecen diversos principios relevantes para concretar el alcance de esta finalidad de creación de un marco de confianza, que son los principios de seguridad y de proporcionalidad, junto a la inevitable referencia a la normativa de protección de datos:

- El principio de protección de los datos de carácter personal, contenido en el punto a), que impone el "respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de Carácter Personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar", normativa cuyo desarrollo ha establecido una importante serie de criterios de seguridad de la información que resultan de obligada aplicación. Sin ánimo de ser exhaustivos, cada vez es más acuciante una revisión de esta normativa, atendiendo al nuevo marco que ha de surgir de la Ley 11/2007, la interoperabilidad entre las Administraciones Públicas que recoge, y que llevará a un previsible aumento de la cesión o comunicación de datos, con o sin consentimiento del titular, lo que nos planteará la captación del mismo por medios electrónicos.
- El principio de seguridad, contenido en el punto f), exige la implantación de "al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa", actuando como límite inferior o mínimo de medidas de seguridad.

- El principio de proporcionalidad, contenido en el punto g), "en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones", actuando como límite superior o máximo de medidas de seguridad para cada procedimiento.

Los anteriores principios encuentran reflejo en el derecho de los ciudadanos a "la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas", recogido en el punto h) del artículo 6 de la LAECSP, así como en los derechos a "obtener los medios de identificación electrónica necesarios" y a "la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas", establecidos en los puntos g) y h) del citado artículo 6 LAECSP.

De la lectura combinada de dichos principios resulta, como se ha apuntado, el necesario establecimiento o determinación de medidas de seguridad a aplicar en los procedimientos administrativos, el cual se ha de basar en el análisis de riesgos y en el empleo de múltiples sistemas técnicos. Esto supone, por una parte, una cierta continuación de los criterios contenidos en la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, pero, por otro lado, finaliza con la tendencia a la adopción de la firma electrónica reconocida como paradigma de la identificación y autenticación.

En efecto, hasta la aprobación de la LAECSP la legislación administrativa establecía la preeminencia de la firma escrita como forma de acreditación de la voluntad, lo que implicaba la adopción de la firma electrónica reconocida - prevista primero en el Real Decreto-Ley 14/1999, de 17 de septiembre, y después en la Ley 59/2003, de 19 de diciembre, de firma electrónica - como mecanismo típico de acreditación electrónica de la voluntad, en aplicación del principio de equivalencia funcional.

A pesar de esta preferencia por la firma electrónica reconocida, cabe indicar que, en la práctica, han existido una gran cantidad de normas que, de un modo u otro, han admitido otras formas de firma electrónica, en especial la firma electrónica avanzada basada en certificado reconocido, sin la exigencia de que la misma fuera producida mediante el empleo de dispositivos seguros de creación de firma. Esta disparidad de criterio se ha manifestado particularmente en el ámbito de las Comunidades Autónomas.

Por el contrario, la LAECSP abandona esa concepción, y se orienta de manera decidida a la admisión del empleo de cualesquiera mecanismos de identificación y autenticación, y de firma electrónica, de acuerdo con los criterios de riesgo que se consideren aplicables.

En este sentido, el artículo 13.2 de la Ley determina que "los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración

determine:

a) En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.

b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.

c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen".

Cabe notar que será cada Administración la que determine los sistemas que podrán ser empleados por los ciudadanos, con la excepción del DNI electrónico, que será de uso obligado en todo caso, como ya se había previsto en la Ley 59/2003, de firma electrónica.

Deben destacarse dos hechos: en primer lugar, que en la segunda opción, prevista en el apartado b), relativa a los sistemas de firma electrónica avanzada, siempre que hayan sido admitidos por las Administraciones Públicas, no parece ser especialmente relevante para su admisión que dicha firma electrónica avanzada se base en un certificado reconocido, como hasta ahora resultaba absolutamente exigible; en segundo lugar, no se garantiza ningún tratamiento privilegiado a la figura de la firma electrónica reconocida, a pesar de que la Ley 59/2003 la configura como la única firma electrónica absolutamente equivalente a la firma escrita.

Se trata de un cambio importante en la orientación de la cuestión hasta la fecha, que obliga a replantear gran parte del debate sobre los tipos y niveles de firma electrónica adecuados para cada procedimiento, pasando de la exigencia de la firma electrónica reconocida en base al principio de equivalencia funcional, a la necesidad de realizar un análisis de riesgo para establecer el nivel de equivalencia material entre el procedimiento presencial existente y su versión electrónica.

La tercera opción contemplada consiste en otros sistemas de firma electrónica, lo que supone la admisión de cualquier otro mecanismo de identificación y autenticación, aunque puedan plantear potenciales problemas de seguridad. Esta posibilidad se encuentra restringida por lo que recoge el artículo 16 LAECSP, que obliga a la Administración que desee emplearlos a tomar en consideración "los datos e intereses afectados, y siempre de forma justificada". Esta obligación supone la necesaria realización de un análisis de riesgos detallado y justificado.

La obligación de admisión de los sistemas de firma electrónica por la Administración competente

Otra de las novedades contenidas en la LAECSP es la obligación de admisión

de los certificados reconocidos por parte de las Administraciones Públicas, que se anuncia en la Exposición de Motivos de la Ley, cuando determina que "también se establece la obligación para cualquier Administración de admitir los certificados electrónicos reconocidos en el ámbito de la Ley de Firma Electrónica".

Esta obligación se concreta en el artículo 13.1 de la Ley, cuando determina que "las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos".

La admisión de certificados se ha configurado como un procedimiento administrativo de carácter decisorio y previo al uso de los certificados emitidos por un prestador de servicios de certificación, que llevan a cabo las Administraciones Públicas, sus organismos autónomos u otras entidades públicas o empresariales vinculadas.

La finalidad del procedimiento de admisión es triple: por una parte, el procedimiento determina la formación y la exteriorización de la voluntad administrativa de hacer uso de la certificación; por otra parte, supone que la Administración, que debe pasar a ser usuaria de los servicios de certificación, comprueba que el prestador ha cumplido de manera efectiva los requisitos establecidos en la Ley 59/2003, de 19 de diciembre, de firma electrónica; finalmente, el procedimiento de admisión de certificados puede servir también para a la Administración para establecer y, posteriormente, comprobar condiciones adicionales al uso de la firma electrónica aplicables al procedimiento concreto de que se trate (o aplicables de forma generalizada a todos los procedimientos de dicha Administración).

De esta forma, el procedimiento de admisión se ha convertido en una condición adicional exigible a los prestadores de servicios de certificación, orientada a la comprobación previa del cumplimiento de la legislación de firma electrónica y, en su caso, de las condiciones adicionales del procedimiento que se hayan establecido.

La necesidad de hacer esta comprobación previa deriva del régimen de libre acceso al mercado que consagran el artículo 3.1 de la Directiva 99/93/CE, de firma electrónica ("los Estados Miembros no condicionarán la prestación de servicios de certificación a la obtención de autorización previa"), y el artículo 5.1 de la Ley 59/2003 ("la prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre concurrencia").

No se puede obviar que este régimen de libre acceso a la actividad de prestador de servicios de certificación supone encontrar, en el mercado, prestadores con diferentes niveles de calidad e, incluso, prestadores que sencillamente incumplen la normativa.

En el fondo del procedimiento de admisión reside, por lo tanto, una auditoría del prestador de servicios de certificación que en algunos casos se delega, en todo

o en parte, a un experto independiente o que puede reenviarse, como veremos posteriormente, a una certificación de la actividad del prestador.

Hay que decir, en cualquier caso, que el procedimiento de admisión no constituye una autorización previa para poder emitir certificados electrónicos al público ni una medida equivalente a ésta, y, caso de que se impongan condiciones adicionales, éstas deben ser objetivas, proporcionadas, transparentes y no discriminatorias.

En el caso de los certificados de persona jurídica, el procedimiento de admisión de certificados es especialmente importante ya que, de acuerdo con el artículo 7.3 de la Ley 59/2003, solo se podrán utilizar "cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones Públicas". Lo mismo resulta en el caso de los certificados de entidad sin personalidad jurídica, en los términos del artículo 15.3 de la LAECSP, que permite la admisión y, por tanto el empleo de estos certificados en todos los procedimientos administrativos, en los términos que determine cada Administración.

Finalmente, cabe recordar que la competencia para dicha admisión se encuentra residenciada en cada Administración Pública usuaria de la firma electrónica. En este sentido, el artículo 15.2 LAECSP establece que "la relación de sistemas de firma electrónica avanzada admitidos, con carácter general, en el ámbito de cada Administración Pública, deberá ser pública y accesible por medios electrónicos. Dicha relación incluirá, al menos, información sobre los elementos de identificación utilizados así como, en su caso, las características de los certificados electrónicos admitidos, los prestadores que los expiden y las especificaciones de la firma electrónica que puede realizarse con dichos certificados".

El servicio de clasificación de evidencias electrónicas de la Agència Catalana de Certificació

En el caso de las administraciones públicas catalanas, el procedimiento de admisión de certificados se ha instrumentado y simplificado con la implantación del servicio de clasificación de la Agencia Catalana de Certificación (CATCert), que informa del grado en que el prestador de servicios de certificación cumple los requisitos legalmente establecidos.

La clasificación de servicios de certificación es un servicio prestado por la Agencia Catalana de Certificación -sin perjuicio de la posible existencia de otros prestadores-, que tiene las siguientes finalidades:

- Facilitar el acceso a las Administraciones Públicas de los servicios de certificación y otros mecanismos de seguridad electrónica, informática y telemática suministrados por prestadores públicos y privados a los interesados, en tres aspectos:

- La clasificación permite el uso de los servicios aunque éstos no dispongan de los certificados necesarios de conformidad, de acuerdo con la normativa de industria, o de acuerdo con un esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información.
- La clasificación permite dotar al servicio de un valor añadido a medida que más Administraciones Públicas catalanas sean usuarias del servicio.
- La clasificación permite abaratar significativamente el coste que supone para el prestador del servicio superar múltiples procedimientos de comprobación del cumplimiento de requisitos para Administraciones Públicas diferentes, o incluso, para departamentos y organismos diferentes de la misma administración.

- Simplificar al máximo el procedimiento de admisión de estos servicios por parte de las administraciones públicas que los deben utilizar, en dos aspectos:
  - La clasificación permite eliminar del procedimiento de admisión la parte relativa a la comprobación del cumplimiento de los requisitos técnicos y jurídicos de carácter general.
  - La clasificación permite admitir más prestadores, y de manera más rápida y barata, pues el listado de prestadores clasificados aumenta sin necesidad de la intervención constante del procedimiento de admisión.

Con la clasificación, que se estructura en niveles de confianza relativos al valor de evidencia que suponen los servicios, los prestadores de servicios presentan sus servicios a CATCert, que los evalúa mediante un procedimiento propio de auditoría en función de una serie de requisitos previamente establecidos, que se encuentran alineados con las normas técnicas nacionales, europeas e internacionales aplicables.

El resultado de la evaluación consiste en la asignación de un nivel de confianza de evidencia electrónica. Los niveles son los siguientes:

- Nivel 0: Evidencia alegada.
- Nivel 1: Evidencia de entidad.
- Nivel 2: Evidencia de origen de datos.
- Nivel 3: Evidencia de autenticidad documental.
- Nivel 4: Evidencia de firma electrónica.
- Nivel 5: Evidencia completa de firma electrónica.

- Nivel 6: Evidencia de larga duración de firma electrónica.

Por su parte, cada Administración Pública, a la hora de regular las condiciones de seguridad de un procedimiento, debe prever la exigencia de una simple identificación (que en su caso podrá también actuar como firma electrónica ordinaria), de una firma electrónica avanzada, de una firma electrónica avanzada basada en certificado reconocido o de una firma electrónica reconocida.

Evidentemente, antes de poder utilizar los mecanismos de firma electrónica, la Administración correspondiente los debe admitir mediante el procedimiento de admisión. En ese momento, la norma reguladora ha de determinar el procedimiento que deberá seguir el interesado para aportar la acreditación del cumplimiento de los diferentes requisitos exigibles, entre los que se puede encontrar haber sido clasificado por la Agència Catalana de Certificació con un nivel concreto.

Por ejemplo, si el análisis de riesgo realizado en relación con un procedimiento concreto requiere de la firma escrita de una persona de manera ineludible y absoluta, o de su equivalente, se puede exigir una firma electrónica reconocida.

En este caso, el interesado podrá emplear cualquier firma electrónica reconocida suministrada por el sector privado siempre que se encuentre en disposición de demostrar fehacientemente que su mecanismo constituye una firma electrónica reconocida. Esta prueba puede ser una certificación del servicio, de acuerdo con la normativa de industria, o bien la clasificación del mecanismo de seguridad con nivel 4.

A título de ejemplo de aplicación del sistema de clasificación, podemos citar el Decreto 96/2004 de la Generalitat de Catalunya, relativo al uso de medios electrónicos, informáticos y telemáticos por la Administración de la Generalitat de Catalunya, que exige el empleo de sistemas de firma electrónica reconocida o de certificados electrónicos con nivel de clasificación 4.

La admisión de la firma electrónica y los sistemas voluntarios de certificación de la actividad de los prestadores de servicios de firma electrónica

La certificación de la actividad del prestador de servicios de certificación es un procedimiento voluntario en virtud del cual una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica el reconocimiento del cumplimiento de los requisitos específicos requeridos en la prestación de los servicios que ofrece al público (artículo 26.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica).

Este procedimiento no es único, ya que la expedición de la certificación la puede realizar una entidad acreditada en el marco de la Ley de industria, pero también puede certificar una entidad sin ninguna acreditación. El artículo 26.2 de la Ley 59/2003 así lo admite, al referirse, entre otros, a la certificación que llevan a cabo las entidades de certificación reconocidas (más correctamente, acreditadas) por las entidades de acreditación designadas de acuerdo con la Ley de industria.

Por lo tanto, debemos distinguir por lo menos dos grados o niveles de certificación de la actividad del prestador de servicios de certificación:

- La certificación del servicio por una entidad de certificación acreditada de acuerdo con la Ley de industria y la normativa de desarrollo posterior.
- La certificación del servicio por otras entidades, de acuerdo con otros criterios, y que ofrece unos beneficios inferiores al anterior.

El primer grado se corresponde con la certificación prevista en el capítulo III del Real decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y la seguridad industrial, que regula la infraestructura acreditable para la calidad.

El segundo grado se corresponde con la definición de unos requisitos y con la ejecución de una auditoría del prestador de servicios de certificación. Esta auditoría se puede ejecutar por una entidad auditora y de inspección acreditada de acuerdo con el Real decreto 2200/1995, o por una entidad sin ninguna acreditación dentro del sistema público, posibilidad que ofrece inferiores garantías formales, pero que favorece más la autorregulación de la industria.

Ambos opciones se pueden considerar sistemas voluntarios de acreditación de acuerdo con la Directiva 99/93/CE, de 13 de diciembre, de firma electrónica, en función de la voluntad de cada Estado Miembro de la Unión Europea, según estos sistemas voluntarios se encuentren alineados con la normativa industrial o, por el contrario, permitan un grado inferior de control público de la actividad de certificación de la actividad de los prestadores de servicios de certificación de firma electrónica.

Actualmente, en el Estado español, no disponemos de ninguna entidad auditora acreditada dentro del sistema industrial. Por este motivo, los únicos sistemas de certificación de prestadores de servicios de certificación disponibles hoy en día son las auditorías hechas por entidades acreditadas o cualificadas de acuerdo con sistemas absolutamente privados, como WebTrust, que ofrece el Instituto de Auditores-Censores Jurados de Cuentas de acuerdo con un contrato de licencia con los Institutos de Auditoría norteamericano y canadiense (AICPA y CICA, respectivamente) y que tiene un gran reconocimiento en el sector privado, y más recientemente, el sello de confianza de prestadores de servicios de certificación de ASIMELEC, notificado a la Comisión Europea de acuerdo con el procedimiento del artículo 11 de la Directiva de firma electrónica, como sistema

voluntario de certificación.

Mientras que el primero se basa en estándares propios del sector financiero producidos en EEUU por el comité X9.79 de ANSI, el segundo se basa en estándares europeos, específicamente diseñados para dar cumplimiento a la Directiva 99/93/CE, de firma electrónica y, en particular, para asegurar la calidad en la expedición de certificados reconocidos de firma electrónica.

Cabe indicar que el servicio de clasificación de la Agència Catalana de Certificació constituye una especie de sistema de certificación en el ámbito público de Cataluña, que podría configurarse como tal al amparo del artículo 26 de la Ley 59/2003, si bien hasta ahora no se ha hecho de esta forma, con la voluntad de aceptar las certificaciones expedidas en otros esquemas de certificación de actividad de los prestadores, como ASIMELEC.

En este sentido, resulta beneficioso estudiar posibles vías de colaboración con dichos esquemas de certificación por parte de los prestadores de servicios relacionados con la firma electrónica.

Como experiencia práctica, se puede indicar que la Agència Catalana de Certificación ha firmado un convenio de colaboración con ASIMELEC, en virtud del cual se reconoce la eficacia de las certificaciones expedidas por ASIMELEC a los prestadores de servicios, que de esta forma obtienen de forma directa y sin mayores trámites la clasificación de la Agència Catalana de Certificació y, en términos prácticos, la admisión de su uso.

Eficacia de los procedimientos de admisión entre diferentes Administraciones Públicas

La obligación de admisión de los sistemas de firma electrónica avanzada se concreta en el artículo 21.1 de la LAECSP, dedicado a la interoperabilidad de la identificación y autenticación por medios electrónicos, que determina que "los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por las Administraciones Públicas como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones Públicas la información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas"; indicando las dos condiciones esenciales para la admisión: viabilidad tecnológica y gratuidad en el uso.

Un posible sentido del texto es que sólo los certificados reconocidos se encuentran cubiertos por la obligación de admisión por las Administraciones Públicas, mientras que otros sistemas de firma electrónica avanzada no gozarían de dicho derecho. Esta interpretación resulta acorde plenamente con la Ley 59/2003, de firma electrónica, dado que los prestadores de servicios de certificación que cumplen los requisitos para suministrar dichos certificados,

especialmente en el caso de la firma electrónica reconocida, tienen la legítima expectativa de que su servicio pueda ser empleado de forma ordinaria en las relaciones entre los ciudadanos (sus clientes) y las Administraciones Públicas.

Sin embargo, a la luz del apartado 2 del artículo 21, otra interpretación posible del texto sería que un certificado reconocido admitido por una Administración Pública deberá ser también admitido por las restantes Administraciones Públicas.

Dicha interpretación se basaría en que dicho apartado 2 determina que "los sistemas de firma electrónica utilizados o admitidos por alguna Administración Pública distintos de los basados en los certificados a los que se refiere el apartado anterior podrán ser asimismo admitidos por otras Administraciones, conforme a principios de reconocimiento mutuo y reciprocidad", y, por lo tanto, a sensu contrario, se debería entender que los sistemas basados en los certificados reconocidos sí deberían ser obligatoriamente admitidos por todas las Administraciones Públicas, desde la admisión por cualquiera de ellas.

Esta segunda interpretación, aún teniendo en cuenta la loable intención que subyace a la misma, podría vulnerar, en nuestra opinión, las competencias de las diferentes Administraciones Públicas en la admisión de sistemas de firma electrónica avanzada, si las condiciones adicionales exigidas para la admisión por las diferentes Administraciones resultan técnicamente diferentes e, incluso, incompatibles, por lo que una vía más adecuada para crear un procedimiento único de admisión frente a todas las Administraciones Públicas debería considerar o construirse sobre la base del empleo de los esquemas nacionales de seguridad y de interoperabilidad como marco de referencia, de acuerdo con el artículo 42 de la Ley 11/2007.