

El pasado 17 de septiembre de 2011 se publicó en el Boletín Oficial del Estado la Instrucción 7/2011, de 15 de septiembre, de la Junta Electoral Central, relativa al procedimiento de acreditación de firmas de apoyo de candidaturas al Congreso de los Diputados, al Senado y al Parlamento Europeo previsto en los artículos 169 y 220 de la Ley Orgánica del Régimen Electoral General. El apartado cinco.6º de la misma dispone que

*"la recogida de avales mediante firma electrónica debe entenderse válida siempre que se ajuste a lo dispuesto por la Ley 59/2003, de 19 de diciembre, de firma electrónica, modificada por la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. En consecuencia, las firmas deberán realizarse con un certificado electrónico de los reconocidos por la Sede electrónica del INE <https://sede.ine.gob.es>. A tal efecto, el representante de la candidatura o de la agrupación de electores deberá comunicar a la Junta Electoral competente el sistema de firma electrónica y de verificación de firma utilizado, que deberá incluir el sello o marca de tiempo en el que se realiza la firma. Se adjunta Anexo con los criterios estadísticos para las certificaciones por muestreo y especificaciones técnicas sobre los sistemas de firma y de verificación admisibles así como el diseño del esquema XML del fichero de firmas."*

Se trata, sin duda alguna, de una medida valiente por parte de la Junta Electoral Central que ha de ser valorada muy positivamente. En efecto, de una parte, la habilitación de sistemas basados en firma electrónica supone que la Administración electoral española se pone a la cabeza en la utilización de medios electrónicos, convirtiéndose así en una referencia incuestionable a nivel internacional. Por otra parte, esta medida contribuirá sin duda a una mejorar sustancialmente la participación directa de los ciudadanos en los asuntos públicos, fortaleciendo así su activo protagonismo en el procedimiento de elección de los representantes democráticos que, en última instancia, podría contribuir notablemente a una mayor regeneración de la actividad política.

En relación con la firma electrónica, la citada Ley 59/2003 autoriza el empleo de diversos tipos de firma electrónica, en su artículo 3 (incluyendo firmas electrónicas basadas en contraseñas, en algoritmos de firma digital, con o sin certificados digitales de identidad, y empleando o no dispositivos seguros de creación de firma electrónica, por lo cual la ley diferencia los efectos jurídicos de la firma electrónica, de la firma electrónica avanzada y de la firma electrónica reconocida), y asimismo crea el DNI electrónico, que contiene un sistema de firma electrónica reconocida que debe ser obligatoriamente aceptado por todas las personas, físicas y jurídicas, públicas o privadas, para cualesquiera trámites (artículo 16).

La Instrucción, sin embargo, limita los sistemas de firma electrónica de la Ley 59/2003 a aquéllos que se basen en un certificado electrónico reconocido en la sede electrónica del INE, en aplicación de la legislación de Administración electrónica, contenida en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, artículos 13.2, 15 y 21.1, limitación que nos resulta razonable.

En este sentido, el artículo 13.2 de la Ley 11/2007 dispone que "los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas [...] a) En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas". Por tanto, al menos el DNI-e debe resultar admitido para la recogida de avales mediante firma electrónica, sin restricciones adicionales.

En relación con los sistemas de firma electrónica diferentes del DNI electrónico, el artículo 21.1 de la Ley 11/2011, dispone 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."

Precisamente dichos certificados admitidos son los que indica la sede electrónica del INE, en cumplimiento de lo dispuesto en el artículo 15.2 de la propia Ley 11/2007 ("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"), por lo que cabe entender que todos estos certificados resultan perfectamente válidos para el procedimiento de recogida de avales.

Sin embargo, continúa la Instrucción diciendo que se incluye anexo con las especificaciones técnicas sobre los sistemas de firma y de verificación admisibles, y sobre el diseño del esquema XML del fichero de firmas, limitando de forma muy importante los formatos y perfiles técnicos de firma a emplear: en concreto, mediante la obligación de uso del formato XAdES incrustada en un documento XML con una sintaxis muy concreta.

De acuerdo con el artículo 4.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, "las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos". Las condiciones adicionales, en virtud del artículo 4.2 de la Ley 59/2003, "serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo", dado el régimen de libre prestación de servicios y no autorización previa en el que se basa la legislación de firma electrónica.

El establecimiento de condiciones adicionales, por tanto, sólo resulta posible cuando exista una justificación objetiva y públicamente comprensible de su necesidad, y cuando no resulte desproporcionada ni arbitraria, impidiendo sin un motivo absolutamente claro. En este sentido, el artículo 21.1 de la Ley 11/2007 establece condiciones que cumplen perfectamente estos criterios, ya que el uso de certificados no reconocidos privaría de posibilidad efectiva de comprobación de la identidad de los avalistas a la Administración electoral. Igualmente, en el supuesto de incompatibilidad técnica para la verificación de los certificados por la citada Administración electoral, o en caso de sometimiento del acceso a la información de verificación a precio, se frustraría la utilidad del sistema de firma, y por tanto se encuentra más que justificada la no admisión de dichos sistemas de firma electrónica.

Sin embargo, la obligación de generación de un formato y perfil técnico de firma electrónica, en un formato sintáctico de documento de aval, que impone la Instrucción no parece encontrar la misma justificación, especialmente porque la Ley 11/2007, y su normativa de desarrollo, han definido de forma minuciosa en qué condiciones puede un ciudadano relacionarse con la Administración, tanto en el Real Decreto 4/2010, de 8 enero, por el que se aprueba el Esquema Nacional de Interoperabilidad como en la Norma Técnica de Interoperabilidad que la desarrolla en materia de firma electrónica, aprobada por Resolución de la Secretaría de Estado para la Función Pública, de 19 de julio (BOE del 30 de julio).

Dicha Norma Técnica recuerda en su exposición de motivos que "el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas", dado que la finalidad del Esquema Nacional de Interoperabilidad es "la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos".

En resumen, "la Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración establece el conjunto de criterios para el desarrollo o adopción de políticas de firma electrónica basada en certificados por parte de las Administraciones públicas. Para ello, define el contenido de una política de firma electrónica basada en certificados, especificando las características de las reglas comunes, como formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos, así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas".

Meridianamente claro resulta el apartado I.2) de la Norma Técnica al reconocer que el contenido de esta NTI será de aplicación para el desarrollo o adopción de políticas de firma electrónica basada en certificados por parte de cualquier Administración Pública. Esto es, la citada Norma Técnica de Interoperabilidad contiene las condiciones para el uso de la firma electrónica, por lo que resulta innecesario que la Instrucción las vuelva a determinar; es más, en caso de que una Administración establezca normas específicas, las mismas deberán necesariamente respetar el contenido de esta Norma Técnica de Interoperabilidad ya que, de lo contrario, se estarían vulnerando injustificadamente los derechos de los ciudadanos.

En efecto, de acuerdo con el apartado III.4.2) de la Norma Técnica de Interoperabilidad, "los formatos para la firma electrónica de contenido, atendiendo a la NTI de Catálogo de estándares, serán:

*"a) XAdES (XML Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2.*

*b) CAAdES (CMS Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.4.*

c) PAdES (PDF Advanced Electronic Signatures), según la especificación técnica ETSI TS 102 778-3”.

Concretando más, el apartado III.4.4.a) de la misma Norma Técnica de Interoperabilidad detalla los tipos de firma admitidas, en relación con el formato documental, incluyendo los siguientes:

- "i. XAdES internally detached signature.
- ii. XAdES enveloped signature.
- iii. CAdES detached/explicit signature.
- iv. CAdES attached/implicit signature.
- v. PAdES."

Como se puede ver, además de la firma XAdES *enveloped* o envuelta, la Norma Técnica de Interoperabilidad concede al ciudadano el derecho al empleo de firmas XAdES *internally detached*; es decir, una firma XAdES completamente separada del documento firmado, pero que se relaciona con el mismo por formar parte de un mismo contenedor, como por ejemplo un fichero ZIP; en el mismo sentido que ha establecido, con carácter obligatorio, la Comisión Europea en su Decisión de 15 de febrero de 2011. En ambos casos, existe para cada aval un documento XML específico, con los datos exigidos por la Instrucción, y la firma electrónica del avalista. La única diferencia entre ambas modalidades es sintáctica, y a los efectos del procedimiento previsto en la Instrucción, manifiestamente irrelevante.

Así pues, dada la íntima vinculación del uso de la firma electrónica para las actuaciones objeto de la referida Instrucción con el ejercicio del derecho fundamental consagrado en el artículo 23.1 de la Constitución Española, habría razones fundadas para considerar que la obligación de uso exclusivo del formato XAdES en su versión "*enveloped*" o incrustada en un documento XML establece una restricción nula de pleno Derecho. En consecuencia, resulta imprescindible que se lleve a cabo una interpretación extensiva de dicha exigencia conforme a las normas constitucionales, legales y reglamentarias referidas ya que, de lo contrario, habría que proceder a la impugnación formal de la Instrucción a fin de garantizar el pleno ejercicio de sus derechos políticos por parte de los ciudadanos.

En definitiva, limitar la presentación de avales a un tipo sintáctico de firma electrónica concreto sin justificación suficiente nos parecería una condición no objetiva, carente de la más mínima proporción y explicación y, en definitiva, claramente discriminatoria. Sobre todo si tenemos en cuenta que los sistemas de verificación de los que se han dotado las Administraciones Públicas y, en concreto, el Ministerio de Política Territorial y Administración Pública, @firma, permiten hoy validar firmas XAdES *internally detached*, así como firmas CAdES en sus dos modalidades, sin dificultad ninguna.

La implementación del sistema que proponemos consiste en remitir a la Junta Electoral, para cada aval, un fichero ZIP que contenga un fichero en XML con el aval, en el formato previsto por la Instrucción, y otro fichero con la firma electrónica XAdES del aval, en modo *internally detached*; esto es, un sistema absolutamente compatible con las necesidades de la Junta Electoral y respetuosa con los derechos de los ciudadanos.