III. OTRAS DISPOSICIONES

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

13171 *Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.*

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad 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, a la vez que redunda en beneficio de la eficacia y la eficiencia.

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.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la norma relativa a las políticas de firma responde a lo previsto en el artículo 18 del citado Real Decreto 4/2010, de 8 de enero, sobre la interoperabilidad en la política de firma electrónica y de certificados.

En particular, 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.

Las condiciones establecidas en esta norma pretenden establecer un marco para la definición de políticas de firma electrónica basada en certificados alineada con las últimas tendencias a nivel europeo como es la Decisión de la Comisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior, compatible a su vez con sistemas de firma electrónica ya implantados.

cve: BOE-A-2011-13171

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración, cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del 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.

Madrid, 19 de julio de 2011.–La Secretaria de Estado para la Función Pública, María Consuelo Rumí Ibáñez.

NORMA TÉCNICA DE INTEROPERABILIDAD DE POLÍTICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS DE LA ADMINISTRACIÓN

ÍNDICE

cve: BOE-A-2011-13171

IV.3 Reglas de confianza para firmas longevas.

Anexo. Etiquetas de creación y validación de firmas electrónicas para los formatos admitidos.

I. *Consideraciones generales*

I.1 Objeto.

1. La Norma Técnica de Interoperabilidad (en adelante, NTI) de Política de firma electrónica y de certificados de la Administración tiene por objeto establecer el conjunto de criterios comunes asumidos por la Administración pública en relación con la autenticación y el reconocimiento mutuo de firmas electrónicas basadas en certificados y que, como tales, serán desarrollados y consolidados a través de las políticas de firma electrónica basada en certificados.

2. El objetivo final de esta NTI es facilitar el uso de firmas electrónicas seguras e interoperables entre las distintas organizaciones de la Administración pública.

I.2 Ámbito de aplicación.

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 órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organizaciones) según el ámbito establecido en el artículo 3 del 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.

II. *La política de firma electrónica*

II.1 Definición y contenido.

1. Según la definición del Real Decreto 4/2010, de 8 de enero, una política de firma electrónica es el «conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma».

2. Una política de firma electrónica y de certificados definirá:

a) Los procesos de creación, validación y conservación de firmas electrónicas.

b) Características y requisitos de los sistemas de firma electrónica, certificados y sellos de tiempo.

3. Toda política de firma electrónica basada en certificados incluirá:

a) Definición del alcance y ámbito de aplicación, que concretará su relación con otras políticas existentes, marco o particulares, así como la identificación de los actores involucrados y los usos de la firma electrónica.

b) Datos para la identificación del documento y del responsable de su gestión.

c) Reglas comunes para el firmante y verificador de la firma electrónica que incluirán:

i. Formatos admitidos de firma electrónica y reglas de uso de algoritmos.

ii. Reglas de creación de firma.

iii. Reglas de validación de firma.

d) Reglas de confianza, que incluirán los requisitos establecidos para certificados, sellos de tiempo y firmas longevas.

e) Otras reglas opcionales a fijar por cada organización, como podrán ser:

i. Reglas específicas de compromisos que cada organización podrá establecer para cada uno de los servicios que presta, estableciendo requisitos específicos necesarios para que la firma sea válida en cada caso.

cve: BOE-A-2011-13171

ii. Reglas de certificados de atributos mediante las que cada organización podrá establecer información adicional a añadir a los certificados digitales en función de sus necesidades y del contexto.

f) Definición de condiciones para el archivado y custodia de firmas electrónicas.
g) Descripción de consideraciones de gestión de la política que se aplicarán a dicho documento.

II.2 Datos identificativos de la política.

1. El documento de política de firma incluirá la siguiente información para su identificación:

a) Nombre del documento.
b) Versión.
c) Identificador (OID-Object IDentifier) de la política.
d) URI (Uniform Resource Identifier) de referencia de la política.
e) Fecha de expedición.
f) Ámbito de aplicación.

2. La política de firma incluirá la definición de su periodo de validez y las consideraciones respecto a los periodos de transición que procedan.
3. Para la identificación de su gestor, la política de firma electrónica basada en certificados incluirá:

a) Nombre del gestor de la política.
b) Dirección de contacto.
c) OID del gestor de la política de firma.

II.3 Actores involucrados en la firma electrónica.

Los actores involucrados en el proceso de creación y validación de una firma electrónica serán:

a) Firmante: persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
b) Verificador: entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política de firma concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.
c) Prestador de servicios de certificación (PSC): Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
d) Emisor y gestor de la política de firma: entidad que se encarga de generar y gestionar el documento de política de firma, por el cual se deben regir el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

II.4 Usos de la firma electrónica.

Las políticas de firma electrónica podrán definir condiciones para la aplicación de una firma electrónica basada en certificados con los siguientes propósitos:

a) Firma de transmisiones de datos, como herramienta para proporcionar seguridad al intercambio, garantizando la autenticación de los actores involucrados en el proceso, la integridad del contenido del mensaje de datos enviado y el no repudio de los mensajes en una comunicación telemática.
b) Firma de contenido como herramienta para garantizar la autenticidad, integridad y no repudio de aquel, con independencia de que forme parte de una transmisión de datos.

cve: BOE-A-2011-13171

II.5 Interacción con otras políticas.

1. Cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente.
2. La definición del alcance y ámbito de aplicación de una política de firma electrónica se realizará considerando su interacción con otras políticas de firma electrónica, y asegurando que:

a) Su desarrollo es interoperable con la política marco, en caso de políticas de firma particulares.
b) Define las condiciones de utilización y convivencia con otras políticas particulares, si se trata de una política marco.

3. En toda política de firma electrónica se asegurará que:

a) Las extensiones o restricciones establecidas para las reglas de creación o validación de firma atienden a la validación de los formatos de firma establecidos en esta NTI y política marco si procede, de forma que se garantice la interoperabilidad entre las diferentes organizaciones.
b) Incluye, si procede, la referencia a la URL de la política marco de firma electrónica en la que se inscribe, con indicación expresa de la versión.
c) Las firmas que se generen siguiendo políticas marco o particulares, incluyen un campo donde se indique de forma explícita la política a la que pertenecen.
d) Para que otras aplicaciones puedan interpretar las reglas de una política particular correctamente, dicha política está disponible en formato XML (eXtensible Markup Language) y ASN.1 (Abstract Syntax Notation One).

II.6 Gestión de la política de firma.

1. La política de firma electrónica incluirá la descripción básica de su proceso de gestión, estableciendo las directrices para su mantenimiento, actualización y publicación, e identificando al responsable de llevar a cabo estas tareas.
2. El gestor de la política de firma mantendrá actualizada la versión de la política de firma atendiendo a:

a) Modificaciones motivadas por necesidades propias de la organización.
b) Cambios en políticas relacionadas.
c) Cambios en los certificados electrónicos emitidos por los prestadores de servicios de certificación referenciados en la política de firma.

3. Para facilitar la validación de firmas electrónicas creadas atendiendo a versiones anteriores de una política, se podrá mantener un repositorio con el historial de versiones anteriores que provea la ubicación de cada versión.

II.7 Archivado y custodia.

1. Atendiendo a las necesidades y normativa específicas de su ámbito, las políticas de firma podrán contemplar la definición de condiciones y responsabilidades para el archivado y custodia de las firmas electrónicas en sus diferentes aplicaciones.
2. Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, se podrán utilizar:

a) Firmas longevas mediante las que se añadirá información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza, aplicando las reglas de confianza para firmas longevas descritas en el subapartado IV.3.
b) Otros métodos técnicos que impedirán la modificación de la firma para la que se ha verificado su validez, de acuerdo a los requisitos establecidos en la política de firma correspondiente, y que habrá sido almacenada en un sistema en un momento del tiempo

cve: BOE-A-2011-13171

determinado. Todos los cambios que se realicen sobre el sistema en el que se encuentra almacenada la firma podrán auditarse para asegurar que dicha firma no ha sido modificada. Los requisitos de seguridad de dichos sistemas cumplirán con las condiciones de los niveles de seguridad establecidos por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3. Cada política de firma definirá un servicio para mantener las evidencias de validez de las firmas longevas y gestionar la actualización de las firmas. Dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma como los certificados e informaciones de estado utilizadas en su validación.

4. El almacenamiento de los certificados y las informaciones de estado podrá realizarse dentro del fichero resultante de la firma electrónica o en un depósito específico:

a) En caso de almacenar los certificados y las informaciones de estado dentro de la firma, se sellarán también dichas informaciones, siguiendo las modalidades de firmas AdES -X o -A.

b) Si los certificados y las informaciones de estado se almacenan en un depósito específico, se sellarán de forma independiente.

5. La protección de la firma electrónica frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez, se realizará a través de uno de los siguientes procesos:

a) Utilización de mecanismos de resellado, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de fecha y hora de archivo con un algoritmo más robusto.

Las políticas de firma podrán definir la aplicación de mecanismos de resellado para facilitar la conservación de la firma electrónica.

b) Almacenamiento de la firma electrónica en un depósito seguro, garantizando la protección de la firma contra falsificaciones y asegurando la fecha exacta en que se guardó la firma electrónica.

Las operaciones de fechado se realizarán con marcas de fecha y hora, no siendo necesario su sellado de tiempo.

6. La definición de medidas y procedimientos para archivado y custodia de firmas electrónicas se realizará atendiendo con proporcionalidad a los diferentes usos de la firma electrónica contemplados en el alcance y ámbito de aplicación de la política.

7. Para archivado y gestión de documentos electrónicos firmados, se atenderá a lo establecido en la NTI de Política de gestión de documentos electrónicos.

III. *Reglas comunes*

III.1 Reglas comunes.

1. Las reglas comunes permitirán establecer responsabilidades respecto a la firma electrónica sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados si son requisitos para el firmante, o no firmados si son requisitos para el verificador.

2. Estas reglas se definirán en base a los formatos de firma electrónica admitidos, teniendo en cuenta los diferentes usos de la firma electrónica basada en certificados, al uso de algoritmos y a los procesos de creación y validación de firma.

III.2 Formatos admitidos de firma electrónica.

1. Los formatos admitidos por las organizaciones para las firmas electrónicas basadas en certificados electrónicos, se ajustarán a las especificaciones de los estándares

cve: BOE-A-2011-13171

europeos relativos a los formatos de firma electrónica así como a lo establecido en la NTI de Catálogo de estándares.

2. Los formatos de firma electrónica serán:

a) Estándares abiertos basados en estándares de firma europeos y ampliamente utilizados.
b) Seleccionados de entre los definidos por la Comisión Europea para la política de interoperabilidad de firmas electrónicas que será regulada a través de Decisión Comunitaria.
c) Compatibles con la definición de políticas de generación y validación de firmas para facilitar la interoperabilidad deseada y el automatismo en el tratamiento de firmas electrónicas generadas por distintas organizaciones.
d) Tales que permitan desarrollar funcionalidades avanzadas como la generación de firmas longevas de cara a garantizar su preservación.
e) Si procede, interoperables con la política marco en la que se basan.

3. Cada organización determinará los formatos y estructuras concretas de firma a incluir en su política, aplicando los criterios expuestos en esta NTI de forma proporcional al uso y necesidades de la firma electrónica en cada caso.
4. Cada organización identificará a la entidad gestora encargada de publicar y actualizar la relación de las especificaciones relativas a los formatos admitidos en su política.
5. La política de firma incluirá los requisitos o, en su caso, procedimientos de actualización, para considerar la inclusión de nuevas versiones de los formatos soportados.

III.3 Formatos de firma electrónica de transmisiones de datos.

1. La firma electrónica de transmisiones de datos estará basada en estándares recogidos en la NTI de Catálogo de estándares, siendo responsabilidad del emisor y gestor de la política la definición de las consideraciones concretas a aplicar por cada organización.
2. Cada política definirá las versiones soportadas así como los cambios en aquellas que pueden provocar una actualización de dicha política.

III.4 Formatos de firma electrónica de contenido.

1. En la política de firma se especificarán los formatos admitidos para la firma electrónica de contenido.
2. 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) CAdES (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.

3. El perfil mínimo de formato que se utilizará para la generación de firmas de contenido en el marco de una política será «-EPES», esto es, clase básica (BES) añadiendo información sobre la política de firma. En cualquier caso, cada organización podrá definir en su política de firma las consideraciones adicionales que considere respecto a la interpretación y utilización de diferentes perfiles y clases de los formatos siempre en consonancia con lo establecido en esta NTI.

cve: BOE-A-2011-13171

4. Las organizaciones aplicarán consideraciones de casos particulares para firma de contenido, al menos, en los siguientes casos:

a) Los documentos electrónicos a los que se aplique firma basada en certificados de cara a su intercambio se ajustarán a las especificaciones de formato y estructura establecidas en la NTI de Documento electrónico.

El formato de firma basada en certificados que acompaña a un documento electrónico se reflejará en el metadato mínimo obligatorio definido en la NTI de Documento electrónico 'Tipo de firma', que, en este caso, podrá tomar uno de los siguientes valores:

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

b) La firma de facturas electrónicas según el formato «Facturae» se realizará conforme a lo regulado por la Orden PRE/2971/2007, de 5 de octubre.

III.5 Reglas de uso de algoritmos.

1. La política de firma especificará las reglas de uso de algoritmos en los diferentes formatos así como la longitud de las claves asociadas a aquéllos de forma proporcional a las necesidades detectadas en los diferentes usos de la firma electrónica, cumpliendo en cualquier caso lo establecido en la NTI de Catálogo de estándares.

2. Para los entornos de seguridad genérica se tomará la referencia a la URN (Uniform Resource Name) en la que se publican las funciones hash y los algoritmos de firma utilizados por las especificaciones XAdES, CAdES y PAdES, como formatos de firma adoptados, de acuerdo con las especificaciones técnicas ETSI TS 102 176-1, «Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms». Todo ello sin perjuicio de los criterios que al respecto se establezcan atendiendo al Real Decreto 3/2010, de 8 de enero.

3. Se admitirán como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en los estándares XML-DSig (XML Digital Signature) y CMS (Cryptographic Message Syntax).

4. Para los entornos de alta seguridad, de acuerdo con el criterio del Centro Criptológico Nacional (CCN) serán de aplicación las recomendaciones revisadas de la CCN-STIC 405 así como en la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía.

5. La definición de usos de algoritmos podrá contemplar diferentes posibilidades según las necesidades en cada caso.

III.6 Reglas de creación de firma electrónica.

1. Las políticas de firma definirán las condiciones particulares bajo las que, en su ámbito, se generará la firma electrónica.

2. Las plataformas que presten el servicio de creación de firma electrónica proporcionarán las funcionalidades necesarias para soportar un proceso de creación de firmas basado en los siguientes puntos:

a) Selección por parte del usuario firmante del fichero, formulario u otro objeto binario para ser firmado. Los formatos de ficheros atenderán a lo recogido en la NTI de Catálogo de estándares.

El firmante se asegurará de que el fichero que se quiere firmar no contiene contenido dinámico que afecte a su validez y que pudiese modificar el resultado de la firma a lo largo del tiempo.

cve: BOE-A-2011-13171

b) El servicio de firma electrónica ejecutará las siguientes verificaciones previas a la creación de la firma:

i. La firma electrónica puede ser validada para el formato del fichero específico que va a ser firmado.
ii. Los certificados a utilizar han sido expedidos bajo una Declaración de Políticas de Certificación específica y son certificados válidos según la legislación aplicable.
iii. Validez del certificado, comprobando si el certificado ha sido revocado, o suspendido, si entra dentro de su periodo de validez, y la validación de la cadena de certificación, incluyendo la validación de todos los certificados en la cadena.

Si alguna de estas verificaciones es errónea, el proceso de firma se interrumpirá.
Si no fuese posible realizar estas comprobaciones en el momento de la firma, será necesario, en todo caso, que los sistemas correspondientes asuman dicha validación, antes de aceptar el fichero, formulario u otro objeto binario firmado.
c) El servicio creará un fichero con la firma según corresponda en función del formato utilizado.
En el momento de la firma, se incluirá la referencia del identificador único de la versión del documento de política de firma electrónica en el que se ha basado su creación.

3. La vinculación del firmante se establecerá a través de etiquetas que, incluidas bajo la firma, y definidas según los estándares correspondientes (XAdES, CAdES y/o PAdES), proporcionarán la siguiente información complementaria a ésta:

a) Fecha y hora de firma, que podrá ser meramente indicativa en función de cómo se haya generado la firma.
b) Certificado del firmante.
c) Política de firma sobre la que se basa el proceso de generación de firma electrónica.
d) Formato del objeto original.

4. Como datos opcionales, la firma electrónica podrá incluir:

a) Lugar geográfico donde se ha realizado la firma del documento.
b) Rol de la persona firmante en la firma electrónica.
c) Acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.).
d) Sello de tiempo sobre algunos o todos los objetos de la firma.

5. La información indicada en los epígrafes 3 y 4 del presente subapartado se recogerá en cada formato de firma según las etiquetas del anexo.
6. En caso de creación de firmas electrónicas por distintos firmantes sobre un mismo objeto, donde el segundo firmante ratifica la firma del primero se utilizará la etiqueta correspondiente, CounterSignature, para contabilizarlas.
7. En el caso de que las múltiples firmas se realicen al mismo nivel, cada una de ellas se representará como una firma independiente.

III.7 Reglas de validación de firma de electrónica.

1. Las políticas de firma definirán las condiciones particulares bajo las que, en su ámbito, será posible validar la firma electrónica de un documento.
2. En el caso de documentos electrónicos, para acceder a la visualización de la firma, el usuario podrá presentar dicho documento electrónico, que contenga los datos, metadatos y firma o firmas, en una sede electrónica o en otros sistemas generales que proporcionen herramientas de reproducción de documentos electrónicos, como el servicio *Valide*, en el *060*.

cve: BOE-A-2011-13171

3. Las condiciones mínimas que se producirán para la validación de la firma serán las siguientes:

a) Garantía de que la firma es válida para el fichero específico que está firmado.
b) Validez de los certificados:

i. El instante de tiempo que se tomará como referencia para la validación será:

1) El momento en que se produjo la firma si se da alguno de los siguientes supuestos:

a) los servicios de los prestadores facilitan los históricos de estado de los certificados y la firma lleva un sello de tiempo válido en el momento de la verificación.
b) se trata de firmas longevas que incluyen las evidencias de la validez de la firma electrónica en el momento de la generación o primera validación, y dichas evidencias se encuentran selladas con un sello de tiempo válido.

2) En otros casos, el momento de la validación.

ii. Se comprobará que los certificados no fueron revocados ni suspendidos y que no han expirado.
iii. Se comprobará la validez de toda la cadena de certificación, incluyendo todos los certificados que la componen, con independencia de que éstos se encuentren incluidos en la propia firma o no.
iv. Se verificará que el certificado ha sido expedido por un prestador de servicios de certificación de confianza bajo una Declaración de Prácticas de Certificación que cumplirá la normativa y estará incluido en la política de firma aplicable.
v. Verificación, si existen y si así lo requiere la política de la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos.

4. Para validar la firma electrónica se considerará la siguiente información:

a) Fecha y hora de la firma: Si se ha realizado el sellado de tiempo, el sello más antiguo dentro de la estructura de la firma se utilizará para determinar la fecha de la firma. En caso de que no existan sellos de tiempo, la fecha y hora de la firma tendrán carácter indicativo, pero no se utilizarán para determinar el momento en que se realizó la firma. En caso de que no existan sellos de tiempo en la firma, la validación del certificado se realizará en el momento de la validación de la firma.
b) Certificado del firmante. Este campo se utilizará para verificar el estado del certificado, y en su caso la cadena de certificación, en la fecha de la generación de la firma.
c) Política de firma sobre la que se basa el proceso de generación de firma electrónica. Se utilizará para identificar, mediante su hash y su identificador (OID), que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que se utilizará para el servicio en cuestión.
Esta validación de la política de firma, implicará que el verificador dispondrá de los medios para verificar las condiciones impuestas en la política de firma concreta. La disponibilidad de la política de firma en un formato interpretable por medios automatizados (XML o ASN.1) y siguiendo los estándares europeos de representación de políticas de firma, indicada en el epígrafe 3.d del subapartado II.5 de esta NTI, facilitará la labor de las aplicaciones receptoras de firmas electrónicas en aplicar distintas políticas de firma.

5. Si se han realizado varias firmas sobre un mismo documento, se seguirá el mismo proceso de verificación que con la primera firma, comprobando cada firma o la etiqueta *CounterSignature* en el campo de propiedades no firmadas, donde se informa de los refrendos de firma generados.

cve: BOE-A-2011-13171

6. El encargado de la verificación de la firma podrá definir sus procesos de validación y de archivado, siempre en consonancia con los requisitos de la política de firma a la que se ajuste el servicio y con lo establecido en la NTI de Política de gestión de documentos electrónicos.

7. Para la verificación del estado de los certificados en el caso de formatos de firma longeva, la validez de la firma vendrá determinada por la validez del sello de tiempo de las evidencias de la validación incluidas en la firma. En estos casos la validez de la firma a lo largo del tiempo se mantendrá resellando la firma antes de la caducidad del certificado de la TSA (Autoridad de sellado de tiempo) que realizó el sello anterior, de forma que siempre sea posible verificar que en el momento en que se realizó la firma, el certificado era válido.

IV. *Reglas de confianza*

IV.1 Reglas de confianza para los certificados electrónicos.

1. Las políticas de firma, marco o particulares, podrán fijar limitaciones y restricciones específicas para los certificados electrónicos que admiten en cada uno de los servicios que corresponda, siempre en consideración de la normativa aplicable en cada caso.

2. Los certificados válidos para ejecutar la firma electrónica de contenido serán los siguientes:

a) Cualquier certificado electrónico reconocido según la Ley 59/2003, de 19 de diciembre, y la Directiva 1999/93/CE, de 13 de diciembre de 1999.

b) Nuevas tipologías de certificados definidos en la Ley 11/2007, de 22 de junio.

3. Los requisitos a cumplir por los prestadores de servicios de certificación en relación con la interoperabilidad organizativa, semántica y técnica serán los establecidos en el artículo 21 de la Ley 11/2007, de 22 de junio, en el artículo 19 del Real Decreto 4/2010, de 8 de enero, y en el resto de normativa aplicable en cada caso.

4. La relación de prestadores de servicios de certificación que emiten certificados reconocidos se podrá consultar en la TSL (Lista de servicios de confianza) publicada en la sede electrónica del Ministerio de Industria, Turismo y Comercio.

5. La política de firma electrónica podrá establecer el período de precaución o de gracia que corresponda aplicar para la validación de los certificados. Este periodo podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (Certificate Revocation Lists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). Esta definición tendrá en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación.

6. El verificador validará los certificados electrónicos en base a los procesos de validación y archivado definidos en la política de firma a la que se ajuste el servicio en cada caso.

IV.2 Reglas de confianza para sellos de tiempo.

1. Los elementos básicos de un sello digital de tiempo serán:

a) Datos sobre la identidad de la autoridad emisora del sello: identidad jurídica, clave pública a utilizar en la verificación del sello, número de bits de la clave, algoritmo de firma digital y función hash utilizados.

b) Tipo de solicitud cursada. Incluyendo, si es un valor resumen o un documento, cuál es su valor y datos de referencia.

c) Valores resumen «anterior», «actual» y «siguiente».

d) Fecha y hora UTC (Universal Time Coordinated).

e) Firma electrónica de todo lo anterior.

cve: BOE-A-2011-13171

2. El sellado de tiempo y la información de validación podrán ser añadidos por el emisor, el receptor o un tercero y se incluirán como propiedades no firmadas en los campos correspondientes según el formato de firma utilizado.

3. En la política de firma se establecerán las condiciones según las que determinar los sellos de tiempo admitidos atendiendo a sus necesidades particulares, y en base a la normativa y legislación vigente. Esto incluye el establecimiento del tiempo máximo aceptable para realizar el sellado de tiempo, anterior, en cualquier caso, a la caducidad del certificado.

4. Los sellos de tiempo seguirán las especificaciones técnicas establecidas en el estándar ETSI TS 102 023, «Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities».

IV.3 Reglas de confianza para firmas longevas.

1. En el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma. En el caso de que sea incluida por el firmante, se podrá realizar una vez haya trascurrido el periodo de precaución o periodo de gracia.

2. Para la conversión de una firma electrónica a firma electrónica longeva:

a) Se verificará la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES y las referencias.

b) Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:

i. Certificados: incluyendo los certificados del firmante y de la cadena de certificación.

ii. Informaciones de estado de los certificados, CRLs o las respuestas OCSP.

c) Aplicación del sellado a las referencias a los certificados y a las informaciones de estado.

3. Para la incorporación a la firma de la información completa de validación, se usará validación mediante CRLs u OCSP.

4. Las políticas de firma contemplarán la definición de formatos y consideraciones de uso de firmas longevas conforme a las necesidades específicas de su ámbito de aplicación y a la normativa específica aplicable.

cve: BOE-A-2011-13171

ANEXO

Etiquetas de creación y validación de firmas electrónicas para los formatos admitidos

Información	Obligatoriedad	Campo – etiqueta – elemento[1]		
		XAdES	CAdES	PAdES
Fecha y hora de la firma	Obligatorio	SigningTime (SignedProperties)	Signing-time (SignedData)	Se indica en el campo "M" del diccionario Signature.
Certificado del firmante	Obligatorio	SigningCertificate (SignedProperties)	ESS signing-certificate ESS signing-certificate-v2 (SignedData)	ESS signing-certificate ESS signing-certificate-v2
Política de firma	Obligatorio	SignaturePolicyIdentifier – SigPolicyId (SignedProperties)	SignaturePolicyIdentifier – SigPolicyId (SignedData)	SignaturePolicyIdentifier
		SignaturePolicyIdentifier – SigPolicyHash (SignedProperties)	SignaturePolicyIdentifier – SigPolicyHash (SignedData)	
Formato del objeto original	Obligatorio	DataObjectFormat (SignedProperties)	Content-hints (SignedData)	No permitido
Lugar geográfico (localización)	Opcional	SignatureProductionPlace (SignedProperties)	Signer-location (SignedData)	Se indica en el campo "Location" del diccionario Signature.
Rol de la persona firmante	Opcional	SignerRole - ClaimedRoles (SignedProperties)	Signer-attributes (SignedData)	Signer-attributes
Acción del firmante sobre el documento firmado	Opcional	CommitmentTypeIndication (SignedProperties)	Commitment-type-indication (SignedData)	Commitment-type-indication
Sello de tiempo	Opcional	AllDataObjectsTimeStamp (SignedProperties)	Content-time-stamp (SignedData)	Content-time-stamp
		IndividualDataObjectsTimeStamp (SignedProperties)		
Contador de firmas electrónicas	Opcional	CounterSignature (UnsignedProperties)	CounterSignature (UnsignedProperties)	No está permitido

[1] Nótese que la tabla no constituye un listado completo de las etiquetas definidas por cada estándar sino una referencia a las etiquetas que reflejarán la información para la creación y validación de la firma.

http://www.boe.es
BOLETÍN OFICIAL DEL ESTADO
D. L.: M-1/1958 - ISSN: 0212-033X