IV. Administración Local

Cartagena

8962 Edicto sobre aprobación definitiva del Reglamento que regula la política de firma y sello electrónicos y de certificados del Excmo. Ayuntamiento de Cartagena.

Visto que con fecha de 30 de junio de 2016 se acordó, por el Excmo. Ayuntamiento Pleno, la aprobación inicial del "Reglamento que regula la política de firma y sello electrónicos y de certificados del Excmo. Ayuntamiento de Cartagena" y que con fecha de 26 de agosto de 2016, se publicó Edicto en el BORM en el que se anunciaba el trámite de información pública por plazo de treinta días del citado Reglamento, sin que se hubiesen presentado alegaciones, es por lo que, habiendo transcurrido el plazo establecido al efecto, de conformidad con lo dispuesto en el artículo 49 de la Ley 7/1985, de 2 de abril, de Bases de Régimen Local, por medio del presente, se acompaña el texto íntegro del "Reglamento que regula la política de firma y sello electrónicos y de certificados del Excmo. Ayuntamiento de Cartagena", para su entrada en vigor de conformidad con los plazos establecidos en los artículos 70.2 y 65.2 de la citada Ley 7/1985, de 2 de abril, entendiéndose definitivamente adoptado el acuerdo de aprobación hasta entonces provisional.

Cartagena, 5 de octubre de 2016. El Concejal Delegado del Area de Hacienda e Interior, Francisco Aznar García.

Reglamento sobre Política de Firma y Sello Electrónicos y de Certificados del Excelentísimo Ayuntamiento de Cartagena.

Tabla de contenido

3.4.3 Reglas para los sellos de tiempo

3.4.4 Reglas de confianza para firmas longevas

3.5 Reglas de confianza para los certificados electrónicos

3.6 Reglas de uso de algoritmos

3.7 Reglas específicas de compromisos

1.- Consideraciones generales

La Ley 59/2003, de 19 de diciembre, de firma electrónica, define la firma electrónica distinguiendo los siguientes conceptos:

· Firma electrónica: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

· Firma electrónica avanzada: es la firma electrónica 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.

· Firma electrónica reconocida: es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Para que una firma electrónica pueda ser considerada firma electrónica avanzada en los términos de la Ley 59/2003 se infieren los siguientes requisitos:

- Identificación: que posibilita garantizar la identidad del firmante de manera única.

- Integridad: que garantiza que el contenido de un mensaje de datos ha permanecido completo e inalterado, con independencia de los cambios que hubiera podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación.

- No repudio: es la garantía de que no puedan ser negados los mensajes en una comunicación telemática.

A ello deben sumarse las modificaciones introducidas por el artículo 5 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información; la implantación del Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE; así como la Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del citado Reglamento. De igual modo, son de aplicación la Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas, y la Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve.

Cuando se firman datos, el firmante indica la aceptación de unas condiciones generales y unas condiciones particulares aplicables a aquella firma electrónica mediante la inclusión de un campo firmado, dentro de la firma, que específica una Política explícita o implícita.

Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa como aplicable, entonces se puede asumir que la firma ha sido generada o verificada sin ninguna restricción normativa, y en consecuencia, que no se le ha asignado ningún significado concreto legal o contractual. Se trataría de una firma que no especifica de forma expresa ninguna semántica o significación concreta y, por lo tanto, hará falta derivar el significado de la firma a partir del contexto (y especialmente, de la semántica del documento firmado).

La finalidad de una Política de firma es reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado, el cual puede ser una transacción determinada, un requisito jurídico o un rol que asuma la parte firmante, entre otros.

Este documento especifica las condiciones generales aplicables a la firma electrónica para su validación, en la relación electrónica del Ayuntamiento de Cartagena y sus organismos públicos vinculados o dependientes con los ciudadanos y entre los órganos y entidades del Ayuntamiento y sus organismos públicos vinculados o dependientes.

1.1 Objeto de la Política

La Política de firma y sello electrónicos y certificados del Ayuntamiento de Cartagena tiene por objeto establecer el conjunto de criterios comunes asumidos por el mismo y sus organismos públicos vinculados o dependientes, en relación con la autenticación y la firma electrónica, que afecta a las relaciones de esta Administración con los ciudadanos y entre sus distintos órganos, según lo previsto en la 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; así como en aquellos artículos de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; y de la Ley 40/2015, del Régimen Jurídico del Sector Público, que la actualizan.

En general, una Política de firma electrónica es un documento legal que contiene una serie de normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal,…), definiendo las reglas y obligaciones de todos los actores involucrados en dicho proceso. El objetivo de este proceso es determinar la validez de la firma electrónica para una transacción en particular, especificando la información que deberá incluir el firmante en el proceso de generación de la firma, y la información que deberá comprobar el verificador en el proceso de validación de la misma.

1.2 Ámbito de aplicación

Este documento se circunscribe a las firmas, los sellos y los certificados previstos en la Ley 59/2003, la Ley 39/2015, la Ley 40/2015, el Reglamento 910/2014 y la Orden PRE/1838/2014 expedidos para su empleo por el Ayuntamiento de Cartagena y los organismos públicos vinculados o dependientes de éste, así como por parte del ciudadano.

2.- La Política de firma y sellos electrónicos

2.1 Alcance de la Política

Este documento propone una Política de firma y sellos electrónicos, que detalla las condiciones generales para la validación de la firma electrónica y una relación de formatos de objetos binarios y ficheros de referencia que deberán ser admitidos por todas las plataformas implicadas en las relaciones electrónicas del Ayuntamiento con los ciudadanos y con las Administraciones Públicas.

La presente Política es de aplicación a todo el Ayuntamiento y sus organismos autónomos y otras entidades dependientes del mismo, y define las 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.

La presente Política también es de aplicación a los documentos resultantes de un proceso de digitalización, de conformidad con lo previsto en la 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 Digitalización de Documentos.

Para su identificación unívoca, la Política de firma dispondrá de un identificador único que podrá ser un OID en ASN.1 o una URI (URL o URN) en XML. El OID o la URI deberán incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente para identificar la Política marco y la versión con las condiciones generales y específicas de aplicación para su validación.

2.2 Datos identificativos de la Política

Se define el identificador de la Política de firma del Ayuntamiento, con el OID [pendiente de definir], o el urn:oid: [pendiente de definir]. Se asignarán identificadores únicos (x.y) para distinguir las versiones sucesivas. También se asignarán identificadores a los distintos formatos de representación (formato legible de PDF, representación en sintaxis XML y representación en sintaxis ASN.1 siguiendo los estándares en sus últimas versiones aprobadas).

La presente Política de firma deberá estar disponible en formato legible, de modo que pueda ser aplicada en un contexto concreto para cumplir con los requerimientos de creación y validación de firma electrónica.

Para facilitar el procesado automático de la firma electrónica, la Política de firma deberá implantarse a su vez en un formato que pueda ser interpretado y procesado automáticamente por los sistemas encargados de la creación y validación de la firma electrónica. Debe estar disponible al menos en formato XML, de acuerdo con el estándar ETSI TR 102 038, o en formato ASN.1, siguiendo el estándar ETSI TR 102 272.

2.3 Actores involucrados en la firma electrónica

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

a) Firmante: una persona física que crea una firma electrónica. Tiene acceso a un dispositivo de creación de firma y actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

b) Creador de un sello: una persona jurídica que crea un sello electrónico.

c) Verificador: entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la presente Política de firma y sello, 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.

d) Prestador de servicios de confianza (PSC): una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.

e) Emisor y gestor de la Política de firma: entidad que se encarga de generar y gestionar el documento de Política de firma y sello, 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.

2.4 Gestión de la Política de firma, sellos y certificados

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al Archivo Municipal y al Centro de Proceso de Datos del Ayuntamiento, previo informe de los Servicios Jurídicos. Los cambios a la Política serán consensuados con las partes implicadas, así como el periodo de tiempo transitorio para la adaptación de las plataformas a la nueva Política.

El Ayuntamiento mantendrá, en los portales destinados a tal función (sede electrónica y portal de transparencia), tanto la versión actualizada del presente documento como un repositorio con el historial de las versiones anteriores de la Política.

En el caso de actualización del presente documento, se identificará el lugar donde un validador puede encontrar las versiones anteriores para verificar una firma electrónica anterior a la Política vigente.

En el momento de la firma se deberá incluir la referencia del identificador único de la versión del documento de Política de firma electrónica sobre el que se ha basado su implantación, el cual determinará las condiciones que debe cumplir la firma electrónica en un momento determinado.

2.5 Archivado y custodia

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, ésta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que para que la firma pueda ser validada a lo largo del tiempo, ésta ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas deberá existir un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables. En lo que concierne a las evidencias electrónicas en vigor en el Ayuntamiento, éstas, así como los procedimientos para su generación, recogida y mantenimiento, quedarán recogidas en documento normativo independiente.

Las condiciones que se deberán dar para considerar una firma electrónica longeva son las siguientes:

1. En primer lugar, deberá verificarse la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES, y las referencias.

2. Deberá realizarse un proceso de completado de la firma electrónica, consistente en lo siguiente:

a. Obtener las referencias a los certificados, así como almacenar los certificados del firmante.

b. Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP (Online Certificate Status Protocol), así como almacenarlas.

3. Al menos, deben sellarse las referencias a los certificados y a las informaciones de estado.

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

· 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 recogidas en la Decisión de la Comisión 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público, o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

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

La protección de la firma/sello electrónico 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:

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

· Se recomienda utilizar mecanismos de resellado/refirma, en el caso de obsolescencia de los algoritmos o formatos, con un algoritmo más robusto.

· Almacenamiento de la firma electrónica en un depósito seguro, que garantice la protección de la firma contra modificaciones y asegurando la fecha exacta en que se guardó la firma electrónica, y en la que se comprobó la autenticidad y vigencia de los elementos que la conforman.

Es necesario que con posterioridad las firmas puedan renovarse (refirmado o countersignature) y permitan actualizar los elementos de confianza (sellos de tiempo), garantizando la fiabilidad de la firma electrónica.

No obstante lo anterior, y de conformidad con lo dispuesto en el artículo 22.4 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, "cuando la

firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos".

Para el archivado y gestión de documentos electrónicos se seguirán las recomendaciones de las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad, aprobado por Real Decreto 4/2010, de 8 de enero.

2.6 Formatos admitidos de firma

El formato de los documentos electrónicos con firma electrónica avanzada, aplicada mediante los certificados electrónicos admitidos por las Administraciones Públicas y utilizados en el ámbito de las relaciones con o dentro del Ayuntamiento, se deberá ajustar a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica. En cualquier caso, el Ayuntamiento admitirá todas las firmas emitidas por autoridades reconocidas de certificación.

Actualmente se consideran formatos admitidos:

· formato XAdES (XML Advanced Electronic Signatures), según especificación técnica ETSI TS 101 903, en su última versión aprobada.

· formato CAdES (CMS Advanced Electronic Signatures), según especificación técnica ETSI TS 101 733, en su última versión aprobada.

· formato PAdES (PDF Advanced Electronic Signatures), según especificación técnica ETSI TS 102 778-3, en su última versión aprobada.

Salvo motivaciones técnicas que lo impidan, como el formato de fichero o el tamaño del fichero de firma resultante, en el Ayuntamiento será de aplicación preferente el formato XAdES, siendo los perfiles admitidos los siguientes:

· XAdES-BES

· XAdES-EPES

· XAdES-T

· XAdES-C

· XAdES-X

· XAdES-X-L

· XAdES-A.

De los citados perfiles, tiene carácter obligatorio la generación de la clase básica –EPES, para todos los documentos que deban firmarse en el contexto del Ayuntamiento y sus organismos autónomos, a la que se añadirá la información –A, para aquellos documentos que deban archivarse a largo plazo. En aquellos casos en que sea preciso utilizar los formatos CAdES o PAdES se seguirá el mismo criterio.

Se tendrá en cuenta la legislación europea en relación a los formatos de firma admitidos en la Unión Europea, en especial aquellos definidos en los estándares europeos de firma electrónica y por tanto deberá ser actualizada según evolucionen dichas normas Europeas. También se tendrá en cuenta la normativa nacional derivada de tal legislación europea. De manera particular, se adoptarán las medidas oportunas para adecuarse a la normativa ya citada:

· Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

· Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público.

· Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

· Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve.

2.7 Creación de la firma electrónica

Las plataformas que presten el servicio de creación de firma electrónica para el Ayuntamiento deberán cumplir las siguientes características:

1. El usuario puede seleccionar un fichero, formulario u otro objeto binario para ser firmado. En el caso de firma de formulario, siempre que sea posible se presentará al usuario el objeto binario a ser firmado, sin necesidad de selección previa.

2. El servicio de firma electrónica ejecutará una serie de verificaciones:

a) Si la firma electrónica puede ser validada para el formato del fichero específico que vaya a ser firmado, según la presente Política.

b) Si los certificados han sido expedidos bajo una Declaración de Políticas de Certificación específica.

c) Comprobación de la validez del certificado: si el certificado ha sido revocado, o suspendido, si entra dentro del periodo de validez del certificado, y la validación.

Si no se pueden realizar estas comprobaciones en el momento de la firma (por ejemplo para firmas en cliente sin acceso a servidor), en todo caso será necesario que los sistemas lo comprueben antes de aceptar el fichero, formulario u otro objeto binario firmado.

Cuando una de estas verificaciones sea errónea, el proceso de firma se interrumpirá.

El fichero de firma resultante debe tener una extensión única de forma que los visores de documentos firmados puedan asociarse a esa extensión, haciendo más fácil al usuario el manejo de este tipo de ficheros. Esta extensión podría ser: o ".xsig", si la firma implantada se ha realizado según el estándar XAdES, o ".csig", si la firma implantada se ha realizado según el estándar CAdES. En el caso de las firmas PAdES, al estar la firma incluida en un documento PDF, la extensión será aquella del formato PDF original.

Todo ello sin perjuicio de la admisión del uso de claves temporales o permanentes por parte de la ciudadanía, así como de otros medios de identificación, como pin del ciudadano o del empleado público, aprobados de

manera formal y explícita por el órgano del Ayuntamiento competente en la materia. En este caso, si el medio de identificación comporta una expresión de voluntad, se entenderá también como medio de firma.

2.8 Verificación de la firma electrónica

El verificador puede utilizar cualquier método para verificar la firma creada según la presente Política. Las condiciones mínimas que se deberán producir para validar la firma serán las siguientes:

1. Garantía de que la firma es válida para el fichero específico que está firmado.

2. Validez de los certificados en el momento en que se produjo la firma, si los servicios de los prestadores facilitan los históricos de estado de los certificados; o, en caso contrario, validez de los certificados en el momento de la validación: certificados no revocados, suspendidos, o que hayan expirado, y la validación de la cadena de certificación (incluida la validación de todos los certificados de la cadena). Esta información puede estar contenida en la propia firma en el caso de las firmas longevas.

3. Certificado expedido bajo una Declaración de Prácticas de Certificación específica.

4. Verificación, si existen y si así lo requiere la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implantados, incluyendo la verificación de los periodos de validez de los sellos.

Puesto que, dependiendo de aspectos como el dispositivo de firma, el momento de la misma, la finalidad de ésta, o el firmante, los datos de contenido del documento pueden ser distintos, el verificador de las firmas debe interpretar el texto firmado para comprobar que se corresponde efectivamente con el documento al que hace referencia la firma. Ello se consigue mediante:

1. La indicación del algoritmo que ha permitido la generación del hash.

2. Los valores de los elementos de metadatos de firma, agente y documento pertinentes, extraídos del esquema de metadatos institucional a aprobar por el órgano competente en la materia del Ayuntamiento.

3. Los valores de los elementos de metadatos y otras evidencias pertinentes, extraídos del documento normativo sobre Política de Evidencias Digitales a aprobar por el órgano competente en la materia del Ayuntamiento.

3. Política de validación de firma electrónica

En este apartado se especifican las condiciones que se deberán considerar por parte del firmante, en el proceso de generación de firma electrónica, y por parte del verificador, en el proceso de validación de la firma.

3.1 Identificación del documento

Nombre del documento	Política de Firma y Sello Electrónicos y de Certificados del Excelentísimo Ayuntamiento de Cartagena
Versión	1
Identificador de la Política	[pendiente de definición, siendo los dos últimos dígitos coincidentes el identificador de versión]
URI de referencia de la Política	[pendiente de definición]
Fecha de expedición	[pendiente de definición]
Ámbito de aplicación	Ayuntamiento de Cartagena y sus organismos autónomos

3.2 Periodo de validez

La presente Política de Firma y Sellos Electrónicos y certificados de la Administración es válida desde la fecha de expedición del apartado anterior hasta la publicación de una nueva versión actualizada, pudiéndose facilitar un periodo de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar las plataformas del Ayuntamiento a las especificaciones de la nueva versión. Este periodo de tiempo transitorio deberá indicarse en la nueva versión, pasado el cual sólo será válida la versión actualizada.

3.3 Identificación del gestor del documento

Nombre del gestor de la Política	Ayuntamiento de Cartagena
Dirección de contacto	C/ San Miguel, 8. 30201 Cartagena (España)

3.4 Reglas comunes

Las reglas comunes para los actores involucrados en la firma electrónica, firmante y verificador, son un elemento obligatorio que debe aparecer en cualquier Política de firma. Permiten 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.

3.4.1 Reglas del firmante

El firmante se hará responsable de que el fichero que se quiere firmar no contiene contenido dinámico que pudiese modificar el resultado de la firma durante el tiempo. Si el fichero que se quiere firmar no ha sido creado por el firmante, deberá asegurarse que no existe contenido dinámico dentro del fichero, como pueden ser macros.

Las reglas específicas para cada formato, son las siguientes:

Formato XAdES

La versión de XAdES contemplada en la presente Política será siempre la última aprobada, siendo válidas implantaciones de versiones anteriores, si ya se hubiera firmado con ellas, y teniendo especial cuidado en indicar en todo momento la versión que se esté utilizando en tags en los que se haga referencia al número de versión. En ningún caso se actualizarán firmas ya aplicadas a documentos a una nueva versión, en el momento de implantar ésta. Las firmas ya aplicadas permanecerán inmodificables.

Para facilitar la interoperabilidad de los sistemas de información que manejan estos documentos firmados electrónicamente, en la generación de firmas XAdES está permitido tanto el uso de estructuras de fichero XML, en las cuales se genere un único fichero resultante que contenga el documento original, codificado en base64, y las firmas, encontrándose al mismo nivel XML lo firmado y la firma, es decir el modo internally detached; como el de estructuras de fichero XML, en las cuales se genere un fichero de firma independiente del documento firmado, que contenga éste codificado en base64 y que se encuentre vinculado a él mediante una referencia, es decir el modo externally detached.

Si el formato del documento original fuese un fichero que contenga sólo texto (fichero XML), no sería precisa su codificación en base64.

De igual modo, en el contexto del Ayuntamiento de Cartagena se permite la firma del hash del documento, sin que resulte precisa la firma del documento

completo en base64, con el objeto de evitar la creación de ficheros de tamaño inmanejable.

Asimismo, se admitirán las firmas XAdES enveloped. En el caso de factura electrónica se acuerda asumir el modo actualmente implementado, mientras se evoluciona a un formato europeo, de acuerdo con el formato Facturae regulado en la Orden PRE/2971/2007; es decir, la firma se considera un campo más a añadir en el documento de factura.

Los ficheros de firma deben proporcionar como mínimo la siguiente información:

· Referencias a los certificados y algoritmos de seguridad utilizados para cada certificado. Este elemento deberá ser firmado con objeto de evitar la posibilidad de sustitución del certificado.

· Identificador de la Política de firma sobre la que se basa el proceso de generación de firma electrónica, y debe incluir los siguientes contenidos en los elementos en que se subdivide:

- Una referencia explícita al presente documento de Política de firma. Para ello, aparecerá el OID que identifique la versión concreta de la Política de firma o la URL de su localización.

- La huella digital del documento de Política de firma correspondiente y el algoritmo utilizado, de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma Política de firma que se utilizara para su validación.

Podrán incorporarse además con carácter opcional los siguientes elementos:

· El lugar geográfico donde se ha realizado la firma del documento.

· La fecha y la hora. En el caso de firma en cliente sin acceder a servidor, será meramente indicativa, pues la fecha en el dispositivo cliente es fácilmente manipulable, y será utilizada con fines distintos a conocer la fecha y hora de firma. En procedimiento independiente, aprobado por el órgano competente en la materia del Ayuntamiento, se determinarán las características y restricciones particulares respecto a generación en cliente de las referencias temporales y sincronización del reloj.

· El formato del documento original, necesario para que el receptor conozca la forma de visualizar el documento.

· La acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.).

· Donde proceda, el rol que la persona desempeña en la firma electrónica. En el caso de su utilización en una factura en formato Facturae, deberá contener uno de los siguientes valores en el campo ClaimedRoles:

- "supplier" o "emisor": cuando la firma la realiza el emisor.

- "customer" o "receptor": cuando la firma la realiza el receptor.

- "third party" o "tercero": cuando la firma la realiza una persona o entidad distinta al emisor o al receptor.

También se permitirá el uso de certificados de atributos para certificar el rol del firmante, en cuyo caso el elemento SignerRole incorporará un elemento CertifiedRoles, que contendrá la codificación en base64 de uno o varios atributos de certificados del firmante. Entre ellos, aunque no con carácter exhaustivo, pueden figurar:

· Pertenencia a empresa o Administración Pública (vincula al empleado con su empresa o Administración, incluyendo el cargo que ostenta).

· Apoderado (la empresa o Administración Pública delimita una serie de poderes específicos al empleado para actuar en su representación. Representación específica).

· Representante (para administradores únicos y representantes con un poder amplio).

· Certificados de facturación electrónica.

· Certificado de servidor seguro.

· Certificado de firma de código.

· Certificado de sellado de tiempo.

La etiqueta CounterSignature, refrendo de la firma electrónica y que se puede incluir en el campo UnsignedProperties, será considerada de carácter opcional. Las siguientes firmas, ya sean en serie o en paralelo, se añadirán de conformidad con lo que indica el estándar XAdES, según el documento ETSI TS 101 903 en su última versión aprobada.

Formato CAdES

En el marco del Ayuntamiento de Cartagena y sus organismos autónomos, el formato CAdES sólo se utilizará en situaciones excepcionales, cuando no sea técnicamente posible u operativo utilizar el formato XAdES. La versión de CAdES será la última aprobada, teniéndose especial cuidado en indicar en todo momento la versión que se esté utilizando en tags en los que se haga referencia al número de versión.

El estándar CMS (Cryptographic Message Syntax) presenta distintas alternativas para la estructura del documento electrónico en relación con la firma electrónica. En la presente Política se adopta el tipo Signed Data con los datos incluidos (attached) para la estructura del documento, especificado en los estándares CMS (IETF RCF 5652) y CAdES (ETSI TS 101 733), que mantiene el documento original y la firma en un mismo fichero.

En el caso de que, debido al tamaño de los datos a firmar, no resulte técnicamente posible o aconsejable realizar las firmas con el formato anteriormente descrito, se generará la estructura de firma detached, que incluye el hash del documento original en la firma.

La firma debe proporcionar con carácter obligatorio la siguiente información:

· El tipo de contenido que debe ser firmado.

· El cifrado del contenido firmado OCTET STRING en encapContentInfo.

· El algoritmo utilizado, como mínimo SHA256 y, siempre que sea posible, SHA512.

· La Política de firma sobre la que se basará la generación de la firma electrónica. El documento deberá incorporar la referencia (OID) a la presente Política, la huella digital del documento de Política y el algoritmo utilizado, de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma Política de firma que se utilizará para su validación.

Con carácter opcional, se puede proporcionar también la siguiente información:

· La fecha y hora de la firma. En el caso de firma en cliente sin acceder a servidor, será meramente indicativa, pues la fecha en el dispositivo cliente es fácilmente manipulable, y será utilizada con fines distintos a conocer la fecha y hora de firma. En procedimiento independiente, aprobado por el órgano competente en la materia del Ayuntamiento, se determinarán las características y restricciones particulares respecto a generación en cliente de las referencias temporales y sincronización del reloj.

· El formato del documento original, siendo su función el que el receptor discierna cómo debe visualizar el documento.

Formato PAdES

En el marco del Ayuntamiento de Cartagena y sus organismos autónomos, el formato PAdES sólo se utilizará en situaciones excepcionales, cuando no sea técnicamente posible u operativo utilizar el formato XAdES. La versión de PAdES será la última aprobada, teniéndose especial cuidado en indicar en todo momento la versión que se esté utilizando en tags en los que se haga referencia al número de versión.

En la versión actual de la presente Política, sólo se considera la posibilidad de utilizar algoritmos RSA para las firmas PAdES.

Las firmas PAdES se generarán en modo PAdES-LTV Profile (Long-Term).

La siguiente información deberá estar firmada y será de carácter obligatorio:

· El tipo de contenido que debe ser firmado.

· El cifrado del contenido firmado OCTET STRING en encapContentInfo.

· El algoritmo utilizado, como mínimo SHA256 y, siempre que sea posible, SHA512.

· El identificador de la presente Política de firma. El documento deberá incorporar el OID de la Política de firma particular aplicada.

Con carácter opcional, se puede proporcionar también la siguiente información:

· La acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.).

· El rol que la persona desempeña en la firma electrónica.

3.4.2 Reglas del verificador

Los atributos que podrá utilizar el verificador para comprobar que se cumplen los requisitos de la presente Política de firma, independientemente del formato utilizado (XAdES, CAdES o PAdES), son los siguientes:

· Signing Time: sólo se utilizará en la verificación de las firmas electrónicas como indicación para comprobar el estado de los certificados en la fecha señalada, ya que únicamente se puede asegurar las referencias temporales mediante un sello de tiempo (especialmente en el caso de firmas en dispositivos cliente). 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.

· Signing Certificate: se utilizará para comprobar y verificar el estado del certificado y, en su caso, la cadena de certificación, en la fecha de la generación de la firma, en el caso que el certificado no estuviese caducado y se pueda acceder a los datos de verificación (CRL, OCSP, etc.), o bien en el caso de que el PSC (Proveedor de Servicio de Certificación) ofrezca un servicio de validación histórico del estado del certificado.

· Signature Policy: se deberá comprobar, que la Política de firma que se ha utilizado para la generación de la firma se corresponde con la que se debe utilizar para un servicio en cuestión.

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

Será responsabilidad del encargado de la verificación de la firma definir sus procesos de validación y de archivado según los requisitos de la presente Política de firma.

Existe un tiempo de espera, conocido como periodo de precaución o periodo de gracia, para comprobar el estado de revocación de un certificado. El verificador puede esperar este tiempo para validar la firma o realizarla en el mismo momento y revalidarla después. Esto se debe a que puede existir una pequeña demora desde que el firmante inicia la revocación de un certificado hasta que la información del estado de revocación del certificado se distribuye a los puntos de información correspondientes. Se recomienda que este periodo, desde el momento en que se realiza la firma o el sellado de tiempo sea, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs o el tiempo máximo de actualización del estado del certificado en el servicio OCSP. Estos tiempos podrán ser variables según el Prestador de Servicios de Certificación.

3.4.3 Reglas para los sellos de tiempo

El sello de tiempo asegura que los datos, la firma del documento que va a ser sellado o la información del estado de los certificados incluidos en la firma electrónica, se generaron antes de una determinada fecha.

Los sellos cualificados de tiempo cumplirán los indicados en el artículo 42.1 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Los elementos básicos de un sello cualificado de tiempo serán los indicados en las Normas Europeas de estandarización:

· ETSI EN 319 422 V1.1.1 Time-stamping protocol and time-stamp token profiles

· ETSI EN 319 421 V1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps o en las que las sustituyan

Los elementos básicos que componen un sello digital de tiempo son:

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

· Tipo de solicitud cursada (si es un valor hash o un documento, cuál es su valor y datos de referencia).

· Parámetros del secuenciador (valores hash "anterior", "actual" y "siguiente").

· Fecha y hora UTC.

· Firma digital de todo lo anterior con la clave pública y esquema de firma digital especificados.

El sellado de tiempo puede ser añadido por el emisor, el receptor o un tercero y se debe incluir como propiedad no firmada en el campo Signature Time Stamp.

El sellado de tiempo debe realizarse en un momento próximo a la fecha incluida en el campo Signing Time y, en cualquier caso, siempre antes de la caducidad del certificado del firmante.

La presente Política admite sellos de tiempo expedidos por prestadores de servicios de sellado de tiempo que cumplan las especificaciones técnicas ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

3.4.4 Reglas de confianza para firmas longevas

Los estándares CAdES, XAdES y PAdES contemplan la posibilidad de incorporar a las firmas electrónicas información adicional para garantizar la validez de una firma a largo plazo, una vez vencido el periodo de validez del certificado. Esta información puede ser incluida tanto por el firmante como por el verificador, y se recomienda hacerlo después de trascurrido el periodo de precaución o periodo de gracia. Existen dos tipos de datos a incluir como información adicional de validación:

· La información del estado del certificado en el momento en que se produce la validación de la firma o una referencia a los mismos.

· Certificados que conforman la cadena de confianza.

En el caso de que sea necesario generar firmas longevas, como mínimo las de aquellos documentos que deban permanecer a largo plazo, se recomienda incluir la información de validación anterior, y añadirle un sello de tiempo. En estos tipos de firma la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

En el caso que se desee incorporar a la firma la información de validación, se usará validación mediante OCSP, ya que mediante este método las propiedades o atributos a incluir son de menor tamaño.

Si la consulta al estado de validación de la firma se realiza mediante un método que resulta en una información muy voluminosa que aumenta de forma desproporcionada el tamaño de la firma, opcionalmente, en lugar de la información de validación indicada anteriormente, se pueden incluir en la firma longeva referencias a dicha información.

Si el archivado de la firma puede comprometer la autenticidad y la evidencia proporcionada por el documento, la firma se archivará de manera independiente y referenciada, y la garantía de las propiedades del documento vendrá dada por su custodia en el archivo, junto con sus metadatos obligatorios.

3.5 Reglas de confianza para los certificados electrónicos

Será responsabilidad del ciudadano firmante asegurarse de que el certificado utilizado para la firma es adecuado para el propósito que lo usa, no pudiendo alegar el propio firmante la invalidez de una firma por el mero hecho de que la DPC (Declaración de Prácticas de Certificación) asociada al certificado electrónico – la cual se indica en su campo "Directivas del certificado"- no recogía el uso que el firmante le dio.

Los certificados válidos para ejecutar la firma/sello electrónicos de contenido serán los certificados electrónicos cualificados de firma y sello según el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de

julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

La relación de prestadores de servicios de certificación que emiten certificados cualificados se consultará en la TSL (Lista de servicios de confianza) publicada en la sede electrónica del Ministerio de Industria, Turismo y Comercio y en las TSL del resto de países de la UE, de conformidad con la Decisión de Ejecución UE 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

3.6 Reglas de uso de algoritmos

Para los entornos de seguridad genérica se tomará la referencia a la URN en la que se publican las funciones de 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 sobre Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature. Todo ello sin perjuicio de los criterios que, al respecto, hayan sido adoptados 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, modificado por el Real Decreto 951/2015, de 23 de octubre, de modificación del 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.

La presente Política admite como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en los estándares XMLDSig y CMS.

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, "Algoritmos y parámetros de Firma Electrónica". Asimismo, para garantizar el cumplimiento del Esquema Nacional de Seguridad, se deberá atender a la recomendación CCN-STIC 807, "Criptografía de Empleo en el ENS".

Se podrán utilizar cualquiera de los siguientes algoritmos para la firma electrónica: RSA/SHA256 y RSA/SHA512 que es el recomendado para archivo de documentos electrónicos (very long term signatures).

3.7 Reglas específicas de compromisos

Previa decisión motivada por parte del órgano competente del Ayuntamiento, se autorizará el uso de sellos de órgano para aquellos que así lo requieran, las condiciones de uso del cual quedarán reflejadas en la propia decisión.

De conformidad con lo prescrito en el artículo 12.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el Ayuntamiento mantendrá un registro de aquellos funcionarios públicos habilitados para prestar asistencia al ciudadano en el uso de medios electrónicos.

De igual modo, de conformidad con lo prescrito en los artículos 5 y 6 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el Ayuntamiento mantendrá un registro de

apoderamientos con la información de obligado cumplimiento, codificada en los mencionados artículos.

4. Actualización

La presente Política se mantendrá revisada y actualizada al menos con carácter anual, y siempre que así lo requiera un cambio en la legislación vigente.

Las actualizaciones de la presente Política serán aprobadas mediante acuerdo de la Junta de Gobierno.

5. Formación

El Ayuntamiento planificará y emprenderá las oportunas acciones formativas para que todos sus empleados, a los niveles pertinentes, estén informados de, cumplan y hagan cumplir la presente Política.

Disposiciones Adicionales:

I.- Sistemas de firma admitidos por el Ayuntamiento de Cartagena

La presente Política se adhiere a los sistemas de firma admitidos por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su Capítulo II; y por la Ley 40/2015, de 1 de octubre, del Régimen Jurídico de las Administraciones Públicas, en sus artículos 40 a 45.

II.- Adecuación

El Ayuntamiento procederá a la implantación de aquellos aspectos que sean de su competencia previstos en la siguiente normativa:

· Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

· Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público

· Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas

· Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve.