DOCUMENTO DE POLÍTICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS EN EL AYUNTAMIENTO DE MADRID

Autor	**Ayuntamiento de Madrid**
Versión	1.0
ID. Documento (OID)	OID 2.16.724.1.8.1.1.1.1.0
URL de referencia de la Política	https://sede.madrid.es
Fecha de expedición	18 de octubre de 2012

ÍNDICE

1 INTRODUCCIÓN

La Ley 59/2003, de 19 de diciembre, define la firma electrónica, estableciendo los conceptos de firma electrónica, firma electrónica avanzada y firma electrónica reconocida.

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (en adelante, LAECSP), contiene la regulación básica de la identificación y autenticación por medios electrónicos de los ciudadanos y de las Administraciones Públicas, previendo la utilización de sistemas de firma electrónica basados en certificados para la identificación de las sedes electrónicas, para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada mediante sellos electrónicos, y para el personal al servicio de las Administraciones Públicas.

En el apartado 1 del artículo 42 de la LAECSP se establece el Esquema Nacional de Interoperabilidad. 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, de tal forma que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos para una mayor eficacia y 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 técnicos sobre diversas cuestiones necesarias para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano.

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.

Esta Norma Técnica de Interoperabilidad de Política de Firma electrónica y de certificados fue publicada el 30 de julio de 2011, BOE nº 182.

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.

El Ayuntamiento de Madrid aprueba, en el Acuerdo de 13 de octubre de 2011 de la Junta de Gobierno de la Ciudad de Madrid, los criterios de implantación, organización y uso de la firma electrónica, se habilita para la elaboración del documento técnico de política de firma y se especifican las condiciones generales aplicables a la firma electrónica. Este Acuerdo es publicado el 17 de octubre de 2011, BOAM nº 6533.

Dicho Acuerdo, en su punto Tercero, establece que el Organismo Autónomo Informática del Ayuntamiento de Madrid elaborará, en el plazo máximo de un año desde la aprobación de este Acuerdo, un documento técnico de política de firma electrónica del Ayuntamiento, entendiendo por tal 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 electrónica.

En el marco legal descrito, el Ayuntamiento de Madrid trata de fijar a través del documento de Política de Firma electrónica y de certificados, y en su ámbito de competencia, las condiciones generales aplicables a la firma electrónica para su validación, y las condiciones

para su uso en la relación electrónica del Ayuntamiento con los ciudadanos, entre los órganos y entidades del Ayuntamiento y con otras Administraciones Públicas.

1.1 Objeto del documento

El objeto del documento de Política de Firma electrónica y de certificados del Ayuntamiento de Madrid es fijar, en su ámbito de competencias, las condiciones generales aplicables a la firma electrónica para su validación y su uso en la relación electrónica del Ayuntamiento con los ciudadanos, entre los órganos y entidades del Ayuntamiento y con otras Administraciones Públicas.

Establece, por tanto, el conjunto de criterios comunes asumidos por el Ayuntamiento de Madrid en relación con la autenticación y el reconocimiento mutuo de firmas electrónicas basadas en certificados.

1.2 Ámbito de aplicación

La presente política de firma será de aplicación, en el ámbito de competencias del Ayuntamiento de Madrid, para los siguientes supuestos:

a) La relación electrónica del Ayuntamiento con los ciudadanos en todos los servicios puestos a disposición de los mismos a través de su Sede electrónica, https://sede.madrid.es.

b) La relación electrónica entre los órganos y empleados del Ayuntamiento, ya sea internamente o con otras entidades externas.

c) La relación electrónica del Ayuntamiento con otras Administraciones Públicas o entidades.

1.3 Normativa y especificaciones técnicas

Se ha considerado como normativa básica aplicable a la materia la siguiente normativa:

• Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (Diario Oficial n° L 013 de 19/01/2000. pág. 12-20).

• Ley 59/2003, de 19 de diciembre, de firma electrónica.

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

• Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

• Real Decreto 1553/2005, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica.

• 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.

• 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.

• Resolución de 19 de julio de 2011, BOE del 30 de julio, 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.

Para el desarrollo del contenido del documento se han tenido en cuenta las siguientes especificaciones técnicas:

- ETSI TS 101 733, v.1.6.3, v1.7.3 y v.1.8.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).

- ETSI TS 101 903, v.1.2.2, v.1.3.2 y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).

- ETSI TS 102 778, v 1.1.2. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic.

- Profile based on ISO 32000-1, Part 3: PAdES Enhanced - PAdES-BES and PAdESEPES Profiles; Part 4: Long-term validation.

- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

- ETSI TS 101 861 V1.3.1 Time stamping profile.

- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.

- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.

- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

- IETF RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

- IETF RFC 3125, Electronic Signature Policies.

- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).

- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

2 POLÍTICA DE FIRMA ELECTRÓNICA

2.1 Definición y contenido

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».

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 debiera incluir el firmante en el proceso de generación de la firma, y la información que debiera comprobar el verificador en el proceso de validación de la misma.

Este documento define, por tanto, los procesos de creación, validación y conservación de firmas electrónicas y las características y requisitos de los sistemas de firma electrónica, certificados y sellos de tiempo usados en el ámbito de actuación del Ayuntamiento.

El documento de Política de Firma electrónica y de certificados del Ayuntamiento de Madrid incluye en los siguientes apartados:

a) Datos para la identificación del Documento de Política de Firma electrónica y de certificados y del responsable de su gestión.

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

- Formatos admitidos de firma electrónica y reglas de uso de algoritmos.
- Reglas de creación de firma.
- Reglas de validación de firma.

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

2.2 Datos identificativos de la política

Se incluye en este apartado la información relativa a la identificación del documento y su periodo de validez, así como la información asociada al órgano responsable de su gestión y actualización.

2.2.1 Identificación del documento

Nombre del documento	Política de firma electrónica y de certificados en el Ayuntamiento de Madrid
Versión	1.0
ID. Documento (OID)	OID 2.16.724.1.8.1.1.1.1.0
URL de referencia de la Política	https://sede.madrid.es
Fecha de expedición	18 de octubre de 2012
Ámbito de aplicación	Ayuntamiento de Madrid

2.2.2 Periodo de validez

La presente Política de Firma electrónica es válida desde la fecha de expedición indicada en apartado anterior hasta la publicación de una nueva versión actualizada. Cada vez que se publique una nueva versión del documento, se indicará su fecha de expedición y su periodo de validez.

2.2.3 Identificación de su gestor

El mantenimiento, actualización y publicación electrónica de los criterios sobre firma electrónica corresponderá al Organismo Autónomo de Informática el Ayuntamiento de Madrid, en coordinación con la Dirección General competente en materia de administración electrónica, en aplicación de sus respectivas competencias, recogidas en sus Estatutos y en el Acuerdo vigente de la Junta de Gobierno de la Ciudad de Madrid, por el que se establece la organización y estructura del Área de Gobierno de Hacienda y Administración Pública y se delegan competencias en su titular y en los titulares de los órganos directivos, respectivamente.

El Ayuntamiento mantendrá en la Sede electrónica la versión actualizada del documento de Política de Firma electrónica y de certificados, con los criterios sobre firma electrónica.

Nombre del gestor de la Política	Informática del Ayuntamiento de Madrid
Dirección de contacto	Albarracín, 33 28037 MADRID
OID del gestor de la política	OID 2.16.724.1.8.2.1.1

2.3 Actores involucrados en la firma electrónica

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

- **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.
- **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.
- **Prestador de servicios de certificación (PSC)**: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- **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.

2.4 Usos de la firma electrónica

Los objetivos en el uso de certificados de firma electrónica son los siguientes:

- En la firma electrónica de transmisión 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.
- En la firma de documentos y contenidos electrónicos, como herramienta para garantizar la autenticidad, integridad y no repudio de los mismos, con independencia de que forme parte de una transmisión de datos.

Los certificados electrónicos de firma podrán ser utilizados, por parte de los ciudadanos y empleados públicos:

a) Como medio de autenticación de la identidad, ya que el Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá, a través de su certificado, acreditar su identidad frente a cualquiera, ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

b) Como medio de firma electrónica de documentos, ya que mediante la utilización del Certificado de Firma (nonRepudition), el receptor de un documento firmado electrónicamente puede verificar la autenticidad de esa firma, pudiendo de esta forma demostrar la identidad del firmante sin que éste pueda repudiarlo.

c) Como medio de certificación de Integridad de un documento, ya que permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación.

2.5 Interacción con otras políticas

El Ayuntamiento de Madrid adopta una política de firma propia según lo establecido en este Documento de Política de Firma y de Certificados. Los criterios técnicos y organizativos de la política de firma en el Ayuntamiento de Madrid se ajustarán a las Normas Técnicas de Interoperabilidad, como desarrollo del Esquema Nacional de Interoperabilidad, y a los criterios técnicos de los formatos y tipos de certificados admitidos, que serán en todo caso publicados y actualizados en la Sede electrónica https://sede.madrid.es.

2.6 Gestión de la política de firma

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al Organismo de Informática del Ayuntamiento de Madrid en coordinación con el Área competente del Ayuntamiento en materia de Administración electrónica. Para ello, los cambios a la política marco serán consensuados con las partes implicadas, así como el periodo de tiempo transitorio para la adaptación de las plataformas a la nueva política marco. El Organismo de Informática del Ayuntamiento de Madrid mantendrá, en la Sede electrónica del Ayuntamiento, https://sede.madrid.es, tanto la versión actualizada del presente documento como un repositorio con el historial de las versiones anteriores de la política de firma electrónica para el Ayuntamiento de Madrid.

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 implementación, el cual determina las condiciones que debe cumplir la firma electrónica en un momento determinado.

2.7 Archivado y custodia

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta 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.

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, 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 recomienda sellar también estas informaciones, siguiendo las modalidades de firmas AdES –X o -A.

- si los certificados y las informaciones de estado se almacenan en un depósito específico, se recomienda sellarlos de forma independiente.

Para proteger la firma electrónica frente a la posible obsolescencia de los algoritmos y poder seguir asegurando sus características a lo largo del tiempo de validez, se deberá seguir uno de los siguientes procesos, de acuerdo con las especificaciones técnicas para firmas electrónicas de tipo CAdES, o XAdES:

- las plataformas de firma electrónica adoptadas en el ámbito del Ayuntamiento de Madrid deberán disponer de mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente.

- la firma electrónica deberá almacenarse 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 criptográfico).

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

Para el archivado y gestión de documentos electrónicos se seguirán las recomendaciones de las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad (RD 4/2010).

3 REGLAS COMUNES

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 Reglas comunes

Las reglas comunes para los actores involucrados en la firma electrónica, firmante y verificador, son un campo 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.

3.1.1 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, se asegurará que no existe contenido dinámico dentro del fichero, como pueden ser macros.

3.1.2 Reglas del verificador

El formato básico de firma electrónica avanzada no incluye ninguna información de validación más allá del certificado firmante, que está incluido en la etiqueta Signing Certificate, y de la política de firma que se indique en la etiqueta Signature Policy.

Los atributos que podrá utilizar el verificador para comprobar que se cumplen los requisitos de la política de firma según la cual se ha generado la firma, independientemente del formato utilizado (XAdES, CAdES o PAdES), son las 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 haya caducado y se pueda acceder a los datos de verificación (CRL, OCSP, etc) o bien en el caso de que el PSC 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.

3.2 Formatos admitidos de firma electrónica

Los formatos admitidos para las firmas electrónicas basadas en certificados electrónicos, se ajustarán a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica así como a lo establecido en la NTI de Catálogo de estándares.

El Organismo de Informática del Ayuntamiento de Madrid será la Entidad gestora encargada de publicar y actualizar la relación de las especificaciones relativas a los formatos admitidos por la presente política de firma.

Actualmente se consideran formatos admitidos:

3.2.1 Formato XAdES (XML Advanced Electronic Signatures)

Según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la versión del estándar nueva a través de una adenda a la política.

• La versión de XAdES empleada en esta política, es la versión 1.3.2, siendo válidas implementaciones según la versión 1.2.2. teniéndose especial cuidado en indicar en todo momento la versión que se esté utilizando en tags en los que se hace referencia al número de versión.

• Para facilitar la interoperabilidad de los sistemas de información que manejan estos documentos firmados electrónicamente, en la generación de firmas XAdES se propone la siguiente estructura de fichero XML, en la cual se genera un único fichero resultante que contiene 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.

```
<documento>
    <documentoOriginal Id=”original” encoding=”base64”
    nombreFichero=nombreFichOriginal”>...
    </documentoOriginal>
    <ds:Signature>
        <ds:SignedInfo/>
        ...
        <ds:Reference URI=”#original”>
        </ds:Reference>
        ...
        </ds:SignedInfo>
```

...

</ds:Signature>

</documento>

Asimismo, se admitirán las firmas XAdES enveloped, dado que es el formato recogido para las facturas electrónicas. En el caso de factura electrónica se acuerda asumir el modo actualmente implementado, 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.

El firmante deberá proporcionar, como mínimo, la información contenida en las siguientes etiquetas dentro del campo SignedProperties (campo que contiene una serie de propiedades conjuntamente firmadas a la hora de la generación de la firma XMLDsig), las cuales son de carácter obligatorio:

- **SigningTime**: indica 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/o será utilizada con fines distintos a conocer la fecha y hora de firma. Las políticas particulares de firma electrónica podrán determinar características y restricciones particulares respecto a generación en cliente de las referencias temporales y sincronización del reloj

- **SigningCertificate**: contiene 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

- **SignaturePolicyIdentifier**: identifica 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, o en su caso, al documento de política de firma particular de cada organismo, en el elemento xades:SigPolicyId. Para ello aparecerá el OID que identifique la versión concreta de la política de firma o la URL de su localización.

    <xades:SigPolicyId>

    <xades:Identifier> ... </xades:Identifier>

    Se admitirá que la firma incluya una referencia implícita a la política de firma siempre que la omisión del identificador de la política no induzca a confusión en cuanto a la política aplicable. En este caso la política aplicable y su versión deberán poder deducirse a partir de otros campos de la firma como el firmante y la fecha de la firma. Por razones de sencillez en la interoperabilidad se recomienda que la política se indique siempre mediante una referencia explícita.

    En todo caso las políticas particulares de firma no podrán referenciarse de forma implícita.

  - La huella digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento <xades:SigPolicyHash>, 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.

- **DataObjectFormat**: define el formato del documento original, y es necesario para que el receptor conozca la forma de visualizar el documento.

Las etiquetas restantes que pueden agregarse en el campo SignedProperties serán consideradas de carácter opcional, sin perjuicio de su consideración obligatoria en políticas particulares, siempre basadas en la política marco o global:

- **SignatureProductionPlace**: define el lugar geográfico donde se ha realizado la firma del documento.

- **SignerRole**: define el rol de la persona en la firma electrónica. En el caso de su utilización, 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.

- **CommitmentTypeIndication**: define la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...).

- **AllDataObjectsTimeStamp**: contiene un sello de tiempo, calculado antes de la generación de la firma, sobre todos los elementos contenidos en ds:Reference.

- **IndividualDataObjectsTimeStamp**: contiene un sello de tiempo, calculado antes de la generación de la firma, sobre algunos de los elementos contenidos en ds:Reference.

• 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 serie o paralelo, se añadirán según indica el estándar XAdES, según el documento ETSI TS 101 903 v1.3.2 (admitiéndose implementaciones según v1.2.2 y posteriores).

3.2.2 Formato CAdES (CMS Advanced Electronic Signatures)

Según especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.3. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la versión del estándar nueva a través de una adenda a la política.

• La versión de CAdES empleada en esta política, es la versión 1.7.3, admitiéndose implementaciones según versión 1.6.3 y posteriores, siempre que no impliquen cambios significativos en los tags empleados. En ese caso, será necesario actualizar el presente documento de Política de Firma electrónica.

• El estándar CMS presenta distintas alternativas para la estructura del documento electrónico en relación con la firma electrónica. Se adopta el tipo Signed Data con los datos incluidos (implícito) 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.

• Las siguientes etiquetas deberán ser firmadas y son de carácter obligatorio:

  - **Content-type**: esta etiqueta especifica el tipo de contenido que debe ser firmado. Es una etiqueta obligatoria según el estándar CAdES.
  - **Message-digest**: identifica el cifrado del contenido firmado OCTET STRING en encapContentInfo. Es una etiqueta obligatoria según el estándar CAdES.

- **ESS signing-certificate o ESS signing-certificate-v2**: es una etiqueta que permite el uso de SHA-1 (sólo para ESS signing-certificate) y la familia de algoritmos SHA-2 como algoritmo de seguridad. Es una etiqueta obligatoria según el estándar CAdES.
- **Signing-time**: indica 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/o será utilizada con fines distintos a conocer la fecha y hora de firma. Las políticas particulares de firma electrónica podrán determinar características y restricciones particulares respecto a generación en cliente de las referencias temporales y sincronización del reloj. Es una etiqueta de carácter obligatorio según está política de firma.
- **SignaturePolicyIdentifier**: es una etiqueta que indica la política de firma sobre la que se basará la generación de la firma electrónica. El documento deberá incorporar la referencia (URL) a la política de firma particular aplicada.
- **Content-hints**: describe el formato del documento original, y su función es que el receptor discierna cómo debe visualizar el documento.

• Las siguientes etiquetas deberán ser firmadas y son de carácter opcional, sin perjuicio de que puedan ser considerados obligatorias en políticas particulares:

- **Content-reference**: puede ser utilizada como un modo de relacionar una contestación con el mensaje original al que se refiere.
- **Content-identifier**: esta etiqueta contiene un identificador que se puede utilizar en el atributo anterior.
- **Commitment-type-indication**: este etiqueta indica la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...).
- **Signer-location**: permite indicar el lugar geográfico donde se ha realizado la firma del documento.
- **Signer-attributes**: indica el rol de la persona en la firma electrónica.
- **Content-time-stamp**: esta etiqueta permite un sello de tiempo, antes de la generación de la firma, sobre los datos que van a ser firmados, para incorporarla con la información firmada.

La etiqueta CounterSignature, refrendo de la firma electrónica, incluido en el campo de propiedades no firmadas, será considerada de carácter opcional. Las siguientes firmas se añadirán según indica el estándar CAdES, según el documento ETSI TS 101 733 v1.7.3 (admitiéndose implementaciones según v1.6.3 y posteriores).

3.2.3 Formato PAdES (PDF Advanced Electronic Signatures)

Según la especificación técnica ETSI TS 102 778-3, versión 1.1.1. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la versión del estándar nueva a través de una adenda a la política o una versión actualizada de la misma..

En el caso de documentos PDF la firma se encuentra embebida en la propia estructura del documento, tal y como especifica el estándar ISO 32000-1:2008.

La estructura de firma para el formato PAdES basada en la norma ETSI TS 102 778-3, incrusta una firma CAdES detached dentro del documento PDF. En este caso, su uso esta fijado por la parte 3 del estándar PAdES “PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles”.

Los perfiles para creación y verificación de firma en documentos PDF, formatos PAdES-BES y PAdES-EPES, tienen características muy similares a los descritos para CAdES, ya que ambos están basados en el estándar CMS.

A esos efectos, aplican los criterios especificados en el apartado 3.2.2 sobre formato CAdES.

El formato PAdES es un formato de firma que aúna la usabilidad y accesibilidad de un PDF junto con la robustez y longevidad de los formatos avanzados (AdES). Es uno de los formatos interoperables propuestos por la Comisión Europea.

Dentro de las distintas clases de los formatos XAdES, CAdES y PAdES, los órganos y unidades administrativas del Ayuntamiento deberán adecuar sus sistemas para la generación de, al menos, la clase básica de uno de estos formatos de firma electrónica, añadiendo información sobre la política de firma (clase EPES), y la verificación de las especificaciones de la clase básica de todos estos formatos.

La clase básica de firma electrónica para definir una política de firma electrónica de interoperabilidad es según los estándares AdES la clase EPES.

Si fuese necesario generar firmas con la intención de validarse a largo plazo, se debería implementar un formato que incorporase propiedades adicionales, como información sobre revocación de certificados.

3.3 Firma electrónica de transmisiones de datos

La firma electrónica de transmisiones de datos estará basada en los estándares recogidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

La firma de transmisiones de datos proporciona integridad, autenticación y no repudio entre dos servidores (punto a punto). En este caso, la firma está asociada al protocolo de transporte, formando parte de los mecanismos de cifrado a implementar en una comunicación segura.

Cuando se implementen mecanismos de transmisión firmada de datos entre el Ayuntamiento de Madrid y otras entidades, que deban cifrarse en una comunicación segura, se hará bajo las especificaciones SOAP, Simple Object Access Protocol, en su versión 1.1., tal y como especifica la Norma Técnica de Interoperabilidad de Catálogo de estándares.

Para transmisiones firmadas de datos basadas en Servicios Web, se aplicarán las firmas electrónicas según el estándar WS-Security: SOAP Message Security de OASIS, versiones 1.0, 1.1 o superiores y, en particular, cumpliendo con la especificación estándar X.509 Certificate Token Profile.

3.4 Firma electrónica de contenido

Los formatos para la firma electrónica de contenido, atendiendo a la Norma Técnica de Interoperabilidad 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, versión 1.1.1.

El perfil mínimo de formato que se utilizará para la generación de firmas de contenido en el marco de la política será «-EPES», esto es, clase básica (BES) añadiendo información sobre la política de firma.

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 Norma Técnica de Interoperabilidad del Documento electrónico, una vez tenido en cuenta el calendario de adaptación de los sistemas del Ayuntamiento de Madrid a las Normas Técnicas de Interoperabilidad.

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

- XAdES internally detached signature.
- XAdES enveloped signature.
- CAdES detached/explicit signature.
- CAdES attached/implicit signature.
- PAdES.

Se describen a continuación los tipos de firma de contenido admitidos:

TIPO DE FIRMA	DESCRIPCIÓN
XAdES internally detached signature	Contenido firmado y firma comparten una misma estructura XML como nodos independientes y del mismo nivel.
XAdES enveloped signature	Contenido firmado y firma comparten una misma estructura XML necesaria para la validación de la firma. La firma se ubica justo después del contenido firmado.
CAdES detached / explicit signature	Contenido firmado y firma constituyen ficheros independientes
CAdES attached/implicit signature.	El fichero de firma envuelve el propio contenido firmado de forma que, para acceder al contenido, es necesario interpretar la firma.
PAdES	Contenido firmado y firma se incluyen bajo un único fichero PDF que permite el acceso a ambos componentes de forma independiente.

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.

3.5 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 pudieran adoptarse como desarrollo del Esquema Nacional de Seguridad, desarrollado a partir del artículo 42 de la Ley 11/2007.

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.

Se podrán utilizar cualquiera de los siguientes algoritmos para la firma electrónica: RSA/SHA1 (formato que se recomienda reemplazar en el medio plazo por algoritmos más robustos),

RSA/SHA256 y RSA/SHA512 que es recomendado para archivado de documentos electrónicos (very long term signatures).

3.6 Reglas de creación de firma electrónica

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

1. El usuario puede seleccionar un fichero, formulario u otro objeto binario para ser firmado (ver Anexo 2 para saber los formatos de ficheros que deberán ser admitidos por las distintas plataformas).

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 o su política de firma particular correspondiente.

   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 de la cadena de certificación (incluidos la validación de todos los certificados en la cadena). 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 es errónea, el proceso de firma se interrumpirá.

El servicio creará un fichero en formato XAdES, CAdES o PAdES para aquellos escenarios en los que sea conveniente.

El fichero 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 será:

- ".xsig", si la firma implementada se ha realizado según el estándar XAdES.
- ".csig", si la firma implementada se ha realizado según el estándar CAdES.
- ".pdf", si la firma implementada se ha realizado según el estándar PAdES.

3. 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.

4. 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:

a) Fecha y hora de 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.

5. 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.

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.

3.7 Reglas de validación de firma electrónica

Las plataformas de validación de firma electrónica del Ayuntamiento de Madrid deberán cumplir las siguientes características:

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).

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 implementados, incluyendo la verificación de los periodos de validez de los sellos.

4 REGLAS DE CONFIANZA

4.1 Reglas de confianza para los certificados electrónicos

El documento de Política de Firma y Certificados indica las limitaciones y restricciones específicas a los certificados electrónicos admitidos para la firma electrónica de contenido en cada uno de los servicios disponibles.

En todo caso, los certificados electrónicos válidos serán:

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) Cualquier nuevo certificado definido y reconocido en la Ley 11/2007, de 22 de junio.

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.

4.1.1 Certificados Admitidos por el Ayuntamiento de Madrid

El Ayuntamiento de Madrid mantendrá actualizada en su Sede electrónica https://sede.madrid.es la relación de certificados admitidos para la realización de trámites, así como los enlaces a la información sobre las políticas de firma y gestión de las diferentes entidades de certificación emisoras de los mismos.

Con carácter básico, para la identificación de ciudadanos y empleados municipales, se admiten los siguientes certificados:

4.1.1.1 DNI electrónico

Política de certificación:

http://www.dnielectronico.es/marco_legal/index.html

4.1.1.2 Fábrica Nacional de Moneda y Timbre

- **Certificado de clase 2 (persona física)**

  El Ayuntamiento de Madrid y la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (en adelante FNMyT-RCM) suscribieron el 5 de diciembre de 2005 un Convenio para la prestación de servicios de certificación de firma electrónica.

  En base a este Convenio, el Ayuntamiento de Madrid ha reconocido el uso de los certificados de clase 2 para personas físicas emitidos por la FNMyT-RCM.

  Estos certificados de persona física contienen, entre otros, los datos identificativos de las mismas. Permiten a los usuarios identificarse y realizar trámites de forma segura con la Administración Pública a través de Internet.

  En el Ayuntamiento de Madrid también se han utilizado para la identificación de los empleados públicos en la tramitación administrativa. Dado que en el Ayuntamiento de Madrid los empleados públicos disponen de una tarjeta criptográfica para su identificación, estos certificados se pueden incorporar en las mismas si se considera necesario.

  Declaración de prácticas de certificación Certificados clase 2:

  http://www.cert.fnmt.es/index.php?cha=cit&sec=3&page=197&lang=es

- **Certificados asociados a servicios avanzados para el entorno de la Administración Pública (AP)**

El Ayuntamiento de Madrid puede utilizar este tipo de certificados emitidos por la FNMyT-RCM para empleados públicos según lo contenido en la adenda al Convenio de fecha 1 de diciembre de 2010.

El Ayuntamiento de Madrid, mediante Acuerdo de 13 de octubre de 2011 de la Junta de Gobierno de la Ciudad de Madrid, BOAM de 17 de octubre, por el que se aprueban los criterios de implantación, organización y uso de la firma electrónica en el Ayuntamiento de Madrid, crea una infraestructura de clave pública (PKI) y establece los criterios de gestión de la misma, para dar cumplimiento a lo fijado respecto a la identificación electrónica de las Administraciones Públicas y autenticación del ejercicio de su competencia en los artículos 13.3 y 17 al 19 de la LAECSP.

Sus políticas y prácticas de certificación asociados están publicadas por la FNMyT-RCM:

Políticas y prácticas de certificación certificados AP:

http://www.cert.fnmt.es/index.php?cha=adm&sec=23&page=224&lang=es

- **Certificado de personal adscrito a la administración o funcionario.**

El Certificado para el personal de la Administración Pública, es la certificación electrónica emitida por la FNMT-RCM que vincula a su titular con unos datos de verificación de firma y confirma, de forma conjunta:

- La identidad de su titular, número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado.
- Al órgano, organismo o entidad de la Administración Pública, bien sea ésta General, autonómica, Local o institucional, donde ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

El ámbito de uso de este tipo de Certificados lo componen las diferentes competencias y funciones propias de los titulares de acuerdo con su cargo, empleo y, en su caso, condiciones de autorización.

Estos certificados pertenecen a AC APE, que esta subordinada a la AC Raíz FNMT-RCM. Se generan en tarjeta criptográfica y tienen una longitud de clave de 2048 bits, siendo su caducidad de 48 meses.

El Ayuntamiento de Madrid, según lo establecido en el Acuerdo de 13 de octubre de 2011 de la Junta de Gobierno de la Ciudad de Madrid, BOAM de 17 de octubre, por el que se aprueban los criterios de implantación, organización y uso de la firma electrónica en el Ayuntamiento de Madrid, está en un proceso de implantación y extensión de estos certificados entre sus empleados públicos.

- **Certificado de sede electrónica,** válidos para la identificación de las sedes electrónicas.

Los Certificados emitidos por la FNMT-RCM para la identificación electrónica de las sedes electrónicas de las administraciones públicas cuya política y Declaración Particular se definen en la DPC de la APE son Certificados Reconocidos según lo definido en la Ley de Firma Electrónica 59/2003 y válidos para la identificación de las sedes electrónicas según lo definido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP)

Los "Certificados de identificación de sede electrónica" son aquellos certificados expedidos por la FNMT-RCM bajo la DPC de la APE y que vinculan unos Datos de verificación de Firma a los datos identificativos de una sede electrónica en la que existe una persona física que actúa como firmante o custodio de la clave y Titular del Certificado, junto con la entidad de la administración a la que pertenece y que es titular de la dirección electrónica a través de la que se accede la sede electrónica (sólo la titularidad es compartida, no siendo así la custodia). Esta persona física es la que tiene el control sobre dicho Certificado y los Datos de creación y verificación de firma y es responsable de su custodia de forma diligente.

Constituyen los límites de uso de este tipo de Certificados la identificación de sedes electrónicas de la Administración Pública, Organismos y entidades públicas vinculadas o dependientes así como el establecimiento de comunicaciones seguras con éstas. La FNMT-RCM y la Administración, organismos y entidades podrán fijar en los acuerdos o convenios, o a través del documento de relación correspondiente o, si fuera procedente en la ley de emisión de estos Certificados, otros límites adicionales.

Estos certificados pertenecen a AC APE, que esta subordinada a la AC Raíz FNMT-RCM. La clave se generará a través de un dispositivo seguro y tendrá una longitud de 2048 bits. La caducidad de estos certificados es de 48 meses.

- **Sello electrónico de órgano,** válidos para la identificación de las unidades responsables en las actuaciones administrativas automatizadas.

El uso principal del sello electrónico de las Administraciones Públicas es la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada y la autenticación de documentos y actuaciones de la Administración, Organismo o Entidad pública titular del mismo. Los certificados de Sello electrónico de las Administraciones Públicas son aquellos certificados expedidos por la FNMT-RCM que vinculan unos datos de verificación de firma a los datos identificativos y de autenticación de determinada Administración, Organismo o Entidad pública y sus respectivas unidades organizativas (unidad que realiza la actuación administrativa automatizada a través de componentes informáticos —área, sección, departamento) y vinculan a la persona física responsable de la Oficina de Registro y/o representante de la Administración, Organismo o Entidad titular del certificado en quien se delegue y que actuarán como custodios del certificado y sus claves.

Estos certificados pertenecen a AC APE, que esta subordinada a la AC Raíz FNMT-RCM. La clave se generará a través de un dispositivo seguro y tendrá una longitud de 2048 bits. La caducidad de estos certificados es de 48 meses.

4.1.2 Código Seguro de Verificación

Según lo establecido en el Artículo 20 del Real Decreto 1671/2009, de desarrollo de la Ley 11/2007, las Administraciones públicas podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas. Dicho código vinculará al órgano u organismo y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

El Ayuntamiento de Madrid ha incorporado a su Sede electrónica un servicio de verificación de documentos electrónicos. El código seguro de verificación debe garantizar el carácter único del código generado para cada documento, así como su vinculación con el documento generado y con el firmante.

El Ayuntamiento de Madrid adaptará el servicio de verificación de documentos de la Sede a las especificaciones de las Normas Técnicas de Interoperabilidad aplicables y publicará en la Sede electrónica la información sobre el uso del servicio y la tipología de los documentos electrónicos accesibles a través del mismo.

4.2 Reglas de confianza para sellos electrónicos de tiempo

El sello electrónico de tiempo asegura que tanto los datos originales del documento que va a ser sellado como la información del estado de los certificados, en caso de que se hayan incluido en la firma electrónica, se generaron antes de una determinada fecha. El formato del sello de tiempo deberá cumplir las recomendaciones de IETF, RFC 5816, “Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP)”.

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

1. 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).

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

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

4. Fecha y hora UTC.

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

El sellado de tiempo y la información de validación pueden ser añadidos por el emisor, el receptor o un tercero y se deben incluir como propiedades no firmadas 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”.

4.3 Reglas de confianza para firmas longevas

Los estándares CAdES (ETSI TS 101 733), XAdES (ETSI TS 101 903) y PAdES (ETSI TS 102 778) 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.

El Ayuntamiento de Madrid implementará en el futuro, e incluirá en el documento de Política de firma electrónica, los mecanismos y criterios de gestión para la firma longeva en documentos y expedientes, una vez que establezca su Política de Gestión Documental, Archivo y Custodia.

En el caso de que se deseen generar firmas longevas, se debe 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.

Al incorporar a la firma la información de validación, se deberá usar 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.

Formato XAdES

Dentro del formato de firma XAdES, el formato extendido XAdES-C incorpora estas entre otras propiedades no firmadas:

- **CompleteCertificateRefs** que contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma, excepto el certificado firmante.

- **CompleteRevocationRefs** que contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación los certificados.

En el caso que se desee incorporar a la firma esta información de validación, se recomienda utilizar el formato **XAdES-X**, que añade un sello de tiempo a la información anterior.

El formato XAdES-XL además de la información incluida en XAdES-X, incluye dos nuevas propiedades no firmadas

- **CertificateValues**

- **RevocationValues**

Estas propiedades incluyen, no solo las referencias a la información de validación sino también la cadena de confianza completa y la CRL o respuesta OCSP obtenida en la validación. Para los atributos CertificateValues y Revocation-Values se recomienda hacer la validación por OCSP ya que estos valores pueden ser muy voluminosos en caso de realizar la validación mediante CRL.

En el caso que se desee incorporar a la firma esta información de validación, se recomienda usar el formato **XADES-A**, que añade un sello de tiempo a la información anterior.

Formato CAdES

Dentro del formato de firma CAdES, el formato extendido CAdES-C incorpora dos atributos:

- **complete-certificate-references** que contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma

- **complete-revocation-references** que contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de la firma.

El formato CAdES-X Long además de la información incluida en CAdES-C, incluye dos nuevos atributos **certificate-values** y **revocation-values** que incluyen, no solo las referencias a la información de validación sino también la cadena de confianza completa y la CRL o respuesta OCSP obtenida en la validación. Para los atributos CertificateValues y Revocation-Values en las firmas longevas se recomienda hacer la validación por OCSP ya que estos valores pueden ser muy voluminosos en caso de realizar la validación mediante CRL

Se recomienda usar los siguientes formatos.

- en el caso que la validación se realice mediante consulta OCSP: los formatos **CAdESX Long type 1 o CAdES-X Long type 2**, que añaden un sellado de tiempo a la información incluida en una firma CAdES X Long. En este caso se incorporan los atributos certificate-values y revocation-values puesto que la respuesta a una consulta OCSP no ocupa mucho espacio.

- en el caso que la validación no pueda realizarse mediante OCSP y se realice mediante consulta a una CRL: los formatos CAdES-X type 1 o CAdES-X type 2, que incluyen un sellado de tiempo a la información incluida en una firma CAdES-C, es decir, a las referencias a las CRL consultada y los certificados de la cadena de confianza. No se recomienda incluir los atributos certificate-values y revocation-values ya que pueden ser muy voluminosos.

En el caso que se esté próximo a la caducidad del sello de tiempo añadido para construir la firma longeva, se puede transformar la firma CAdES-X Long type 1 o CAdES-X Long type 2, en una firma **CAdES-A**, añadiendo un sellado de tiempo de archivo a la firma anterior.

Formato PAdES

- en el caso de forma PAdES se recomienda el uso del formato PAdES-Long Term.

- Igual que en casos anteriores, se recomienda usar validación mediante OCSP, ya que el tamaño de la información de validación a añadir es menor.

- Además, se podría añadir un sello de tiempo que incluyese dicha información de validación ya que la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

5 ANEXO I: ETIQUETAS DE CREACIÓN Y VALIDACIÓN DE FIRMAS ELECTRÓNICAS PARA LOS FORMATOS ADMITIDOS

Este punto muestra las etiquetas que deben ser utilizadas para reflejar la información del firmante establecida como obligatoria u opcional en el punto 3.2 de "Formatos admitidos de firma electrónica", así como para la validación de la firma electrónica en cada uno de los formatos admitidos según las condiciones establecidas en la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados.

No se incluyen por tanto la definición completa de las etiquetas de creación y validación de firmas electrónicas para los formatos admitidos definidas por cada estándar, sino que se limita a citar aquellas relacionadas con la información de firma mencionada a lo largo del documento de Política de firma electrónica y de certificados del Ayuntamiento.

Información	Obligatoriedad	Campo – etiqueta – elemento[3]		
		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

Información	Obligatoriedad	Campo – etiqueta – elemento[3]		
		XAdES	CAdES	PAdES
Acción del firmante sobre el documento firmado	Opcional	CommitmentTypeIndication (SignedProperties)	Commitment-type-indication (SignedData)	Commitment-type-indication
Sello de tiempo	Opcional	AllDataObjectsTimeStamp (SignedProperties) IndividualDataObjectsTimeStamp (SignedProperties)	Content-time-stamp (SignedData)	Content-time-stamp
Contador de firmas electrónicas	Opcional	CounterSignature (UnsignedProperties)	CounterSignature (UnsignedProperties)	No está permitido

6 ANEXO II: FORMATO DE FICHEROS Y OBJETOS BINARIOS ADMITIDOS

Este marco de condiciones generales sobre los formatos de fichero de referencia a admitir por las plataformas de relación electrónica del Ayuntamiento de Madrid con los ciudadanos y con las Administraciones públicas pretende establecer unas consideraciones generales, así como la relación de formatos de fichero y objetos binarios que deberán ser admitidos por todas las plataformas para facilitar su interoperabilidad. No obstante lo anterior, estas plataformas podrán admitir otros formatos de acuerdo con las necesidades específicas que en cada caso se planteen.

La relación completa de las condiciones generales en materia de formatos de fichero se ajustarán a las establecidas por las Normas Técnicas de Interoperabilidad que desarrollan el Esquema Nacional de Interoperabilidad y, en concreto, los formatos y criterios recogidos en la Norma Técnica de Interoperabilidad de Catálogo de Estándares.

6.1 Consideraciones generales

• Los formatos de los documentos electrónicos admitidos no deberán obligar a disponer de licencias para visualizarlos o imprimirlos en diferentes sistemas operativos. Se evitarán en la medida de lo posible los formatos propietarios, porque no es posible asegurar la supervivencia de la empresa. En este sentido, la adhesión a los estándares internacionales es un requisito para la disponibilidad a largo plazo de un documento electrónico.

• Se dispondrá de la posibilidad de comprobar automáticamente el formato y su versión antes de admitirlo en el sistema, es decir, sólo se admitirán ficheros cuyo formato pudiera ser comprobado por una máquina antes de su aceptación.

• Sólo se admitirán formatos estables que gozaran de la aceptación general y tuvieran una expectativa de vida larga. La evolución de los formatos debería mantener compatibilidad con los formatos anteriores.

• Habría que evitar documentos que tuvieran enlaces a otros documentos externos ya que debieran ser autocontenidos. Se considerará como una excepción el caso de los esquemas de validación asociados a formatos XML.

• Debido al riesgo de introducción de código malicioso, se deberá tener especial precaución con aquellos que contengan código ejecutable, como pueden ser macros. La documentación que se presente deberá estar libre de virus informáticos.

En todo caso, el Ayuntamiento de Madrid, mantendrá actualizada en su Sede electrónica https://sede.madrid.es la relación de formatos de ficheros y objetos binarios admitidos para cada servicio, así como las limitaciones técnicas o de tamaño que puedan aplicar.