Paterna

informatica@ayto-paterna.es

Área de Organización y Modernización-TIC
Clasificación: 6.3.6
Expte: 11/15

EDICTO

Mediante Decreto de Alcaldía nº 2.119, dictado en fecha 1 de Junio de 2016, se procede a la aprobación de la Política de Firma Electrónica y de Certificados del Ayuntamiento de Paterna y, en cumplimiento de lo en él resuelto, se procede a publicar su contenido del siguiente tenor literal:

"EVA PÉREZ LÓPEZ, Teniente de Alcalde del Ayuntamiento de Paterna (Valencia), delegada en materia de Tecnologías de la Información y Modernización, en virtud de las atribuciones que me confiere el Decreto de Alcaldía nº 3.460, de fecha 21 de Octubre de 2015, publicado en el BOP nº 212 de fecha 4 de Noviembre de 2015, vengo en dictar el siguiente DECRETO:

Dada cuenta del expediente iniciado para la implantación de un sistema de interoperabilidad y para la adecuación de los sistemas y servicios al Esquema Nacional de Interoperabilidad.

RESULTANDO que la cooperación entre las Administraciones Públicas es esencial para proporcionar los servicios a los ciudadanos y garantizarles su derecho a relacionarse con ellas por medios electrónicos. Dicha cooperación requiere unas condiciones tales que permitan que la misma se pueda llevar a cabo con fluidez para lo cual es necesario que haya interoperabilidad.

RESULTANDO que la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, establece la contribución de la interoperabilidad a la realización del derecho de los ciudadanos a comunicarse con las Administraciones Públicas a través de medios electrónicos; y su artículo 42 crea el Esquema Nacional de Interoperabilidad (en adelante, ENI).

RESULTANDO que este precepto define en el apartado 1 el ENI, como *"… el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deben ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad".*

RESULTANDO que, por otro lado, el ENI establece la serie de Normas Técnicas de Interoperabilidad (en adelante, NTI) que son de obligado cumplimiento por las Administraciones Públicas y que desarrollan aspectos concretos de la interoperabilidad entre éstas y con los ciudadanos.

RESULTANDO que se emiten informes por la Jefa de Área de Organización y Modernización-TIC en fecha 28 de Enero y 25 de Mayo de 2016, elevando a la Alcaldía la Política de firma electrónica y certificados para su aprobación.

RESULTANDO que, en atención a las guías de aplicación y otros documentos de apoyo de las NTI, editados por la Secretaría de Estado de Administraciones Públicas, se ha elaborado la siguiente Política prevista en el ENI, la cual figura como Anexo al presente acuerdo para su aprobación:

Política de firma electrónica y certificados.- La *Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración*, se aprobó por la Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública. Esta 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.

RESULTANDO que, a estos efectos, el Ayuntamiento de Paterna ha elaborado y traslada a aprobación, mediante el presente, su *Política de firma electrónica y certificados*.

RESULTANDO que la Política define el contenido de una política de firma electrónica basada en certificados, especificando las características de las reglas comunes, como formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos, así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas.

RESULTANDO que las condiciones establecidas en la Política pretenden establecer un marco para la definición de políticas de firma electrónica basada en certificados alineada con las últimas tendencias a nivel europeo como es la Decisión de la Comisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo

relativa a los servicios en el mercado interior, compatible a su vez con sistemas de firma electrónica ya implantados.

CONSIDERANDO que por el Área de Organización y Modernización TIC, se pone en conocimiento de la Alcaldía, los siguientes documentos elaborados y publicados en el Portal de Usuarios de informática, de acuerdo con otras NTI del ENI, y que servirán de guía u orientación a la instauración de la Administración electrónica en el Ayuntamiento de Paterna:

a. Expediente electrónico.- Se ha definido la estructura de los expedientes electrónicos, que incluye documentos electrónicos, índice electrónico, firma electrónica y metadatos mínimos obligatorios, así como las especificaciones para los servicios de remisión y puesta a disposición; para los aspectos relativos a la gestión y conservación de los expedientes electrónicos se remite a la *NTI de Política de gestión de documentos electrónicos*. Este documento se ha elaborado de acuerdo a la NTI específica, aprobada por la Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública.

b. **Documento electrónico.-** Se ha definido las condiciones técnicas mínimas necesarias para permitir un intercambio de documentos electrónicos normalizado. Más específicamente, se definen los componentes del documento electrónico, incluyendo contenido, firma electrónica y metadatos mínimos obligatorios, y su formato, así como las condiciones para su intercambio y reproducción; para los aspectos relativos a la gestión y conservación de los documentos electrónicos se remite a la *NTI de Política de Gestión de Documentos Electrónicos*; finalmente se incluye en anexo la definición de metadatos mínimos obligatorios, los esquemas XML para intercambio de documentos y la información básica de firma de documentos electrónicos: En este sentido, la estructura del documento electrónico definida permite la utilización de firmas electrónicas, en un tratamiento de documentos transfronterizo. Este documento se ha elaborado de acuerdo a la NTI específica, aprobada por la Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública.

c. **Procedimientos de digitalización.-** Acorde con la *Norma Técnica de Interoperabilidad de Digitalización de Documentos*, aprobada por la Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, se han definido unos *procedimientos de*

digitalización, en los que se establece los componentes de un documento electrónico digitalizado, incluyendo la imagen electrónica, firma electrónica y metadatos, así como las reglas para la digitalización de documentos en soporte papel por parte del Ayuntamiento, atendiendo a los formatos, niveles de calidad, condiciones técnicas y estándares aplicables.

d. **Catálogo de Estándares.-** Acorde a la *Norma Técnica de Interoperabilidad de Catálogo de estándares*, aprobada por la Resolución de 3 de octubre de 2012 (BOE 31 de octubre), de la Secretaría de Estado de Administraciones Públicas, se ha definido un *Catálogo de estándares* formado por un conjunto mínimo de estándares que satisfacen lo previsto en el artículo 11 del Real Decreto 4/2010, de 8 de enero. Asimismo, establece condiciones necesarias para su revisión y actualización, en el uso de estándares no incluidos en este Catálogo.

e. **Procedimientos de copiado auténtico y conversión entre documentos electrónicos,** así como desde papel u otros medios físicos a formatos electrónicos.- Acorde a la *Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos,* aprobada por la Resolución de 19 de Julio de 2011 (BOE de 30 de julio) de la Secretaría de Estado para la Función pública, en ella se establece las condiciones para la obtención de copias electrónicas auténticas y las copias papel de documentos públicos administrativos desarrollando lo establecido en el artículo 30 de la Ley 11/2007 y para la conversión entre documentos electrónicos atendiendo a la necesidad de preservar la conservación, acceso y legibilidad de los documentos electrónicos según en el artículo 23 del R.D 4/2010, de 8 de Enero.

CONSIDERANDO el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, por el se crea el ENI.

CONSIDERANDO lo dispuesto en el artículo 1 del R.D. 4/2010, de 8 de Enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, en relación con la garantía de interoperabilidad.

CONSIDERANDO el artículo 18.2 del citado Real Decreto, en cuanto a la aprobación de la Política de firma electrónica y de certificados.

CONSIDERANDO que, de conformidad con la Disposición Adicional Primera *"Desarrollo del Esquema Nacional de Interoperabilidad"*, se desarrollarán las NTI que serán de obligado cumplimiento por parte de las Administraciones Públicas.

CONSIDERANDO los informes emitidos por la Jefa de Área de Organización y Modernización-TIC en fecha 28 de Enero y 25 de Mayo de 2016, elevando la referida Política a la Alcaldía para su aprobación.

CONSIDERANDO que este órgano es competente para resolver, de conformidad con lo previsto en el artículo 21 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

CONSIDERANDO la delegación de atribuciones efectuada en la Tenencia de Alcaldía de Sostenibilidad y Atención a la Ciudadanía por la Alcaldía mediante Decreto nº 3.410, de fecha 21 de Octubre de 2015, publicado en el BOP nº 212 de fecha 4 de Noviembre de 2015.

CONSIDERANDO el informe-propuesta emitido por la Jefa de Área de Promoción y Dinamización Municipal.

En base lo expuesto, esta Tenencia de Alcaldía RESUELVE:

PRIMERO.- Aprobar la Política de firma electrónica y de certificados del Ayuntamiento de Paterna, de conformidad con el artículo 18 del Real Decreto 4/2010, de 8 de enero, cuyo documento firmado electrónicamente obra en el expediente y cuyo texto íntegro se transcribe como Anexo.

SEGUNDO.- Dar cuenta de la documental relativa al Esquema Nacional de Interoperabilidad, editada y elaborada acorde a las guías de las Normas Técnicas de Interoperabilidad, aprobadas por las diferentes resoluciones de la Secretaría de Estado para la Función Pública.

TERCERO.- Publicar la indicada normativa en el Portal de Usuarios TIC, a los efectos oportunos.

CUARTO.- Ordenar la publicación del presente acuerdo en el Boletín Oficial de la Provincia de Valencia.

QUINTO.- Determinar que el presente acuerdo entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Provincia de Valencia.

Paterna

informatica@ayto-paterna.es

ANEXO

POLÍTICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS EN EL AYUNTAMIENTO DE PATERNA

INDICE

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.

- **Firma electrónica general: "**La 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: "**Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma".

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.

De conformidad con el marco legal descrito, el Ayuntamiento de Paterna 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.

La presente Política, está elaborada acorde con la **GUÍA DE APLICACIÓN DE LA NTI – POLÍTICA DE FIRMA ELECTRÓNICA Y CERTIFICADOS DE LA ADMINISTRACIÓN**, publicada por la Dirección General para el Impulso de la Administración Electrónica. 1ªedición electrónica – Versión 01/09/2011.

1.1 Objeto del documento

El objeto del documento de Política de Firma electrónica y de certificados del Ayuntamiento de Paterna 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 Paterna 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 Paterna, 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://sedepaterna.sede.dival.es/opencms/opencms/index.html

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 términos generales una política de firma electrónica 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 Paterna 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 área u órgano responsable de su gestión y actualización.

2.2.1 Identificación del documento

Nombre del gestor de la Política	Política de firma electrónica y de certificados en el Ayuntamiento de Paterna
Versión	1.0
ID. Documento (OID/Object IDentifier)	2.16.724.1.11.1.1.1.1.0
URI (Uniform Resource Identifier) de referencia de la Política (URL sede electrónica)	https://sedepaterna.sede.dival.es/opencms/opencms/index.html
Fecha de expedición	28 enero 2015
Ámbito de aplicación	Ayuntamiento de Paterna

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.

2.2.3 Identificación de su gestor

El mantenimiento, actualización y publicación electrónica de los criterios sobre firma electrónica corresponderá al Área de Organización y Modernización TIC del Ayuntamiento de Paterna.

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	Área de Organización y Modernización-TIC del Ayuntamiento de Paterna
Dirección de contacto	Plaza Enginyer Castells, nº1 - 46980 Paterna (Valencia)
OID (Object IDentifier) del gestor de la política	2.16.724.1.11.2.1

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/Firma digital) 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 (non Repudition/**no Repudio**), 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 Paterna 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 Paterna 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://sedepaterna.sede.dival.es/opencms/opencms/index.html

2.6 Gestión de la política de firma

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al Área de Organización y Modernización TIC del Ayuntamiento de Paterna, en coordinación con el Comité de Seguridad, competente en materia de seguridad para la administración electrónica del Ayuntamiento.

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 Área de Organización y Modernización TIC del Ayuntamiento de Paterna del Ayuntamiento de Paterna mantendrá, en la Sede electrónica del Ayuntamiento, https://sedepaterna.sede.dival.es/opencms/opencms/index.html, 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 Paterna.

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[1].
- si los certificados y las informaciones de estado se almacenan en un depósito específico, se recomienda sellarlos de forma independiente.

[1] Existen distintos formatos de firma que van incrementando la calidad de la misma hasta conseguir una firma que pueda ser verificada a largo plazo (de forma indefinida) con plenas garantías jurídicas:

Firma Básica (AdES – BES), es el formato básico para satisfacer los requisitos de la firma electrónica avanzada.

AdES T, se añade un sellado de tiempo (T de TimeStamp) con el fin de situar en el tiempo el instante en que se firma un documento.

AdES C, añade un conjunto de referencias a los certificados de la cadena de certificación y su estado, como base para una verificación longeva (C de Cadena).

AdES X, añade sellos de tiempo a las referencias creadas en el paso anterior (X de eXtendida).

AdES XL, añade los certificados y la información de revocación de los mismos, para su validación a largo plazo (XL de eXtendido Largo plazo).

AdES A, permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada o guardada para futuras verificaciones (A de Archivo).

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 Paterna 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 área de Organización y Modernización TIC del Ayuntamiento de Paterna 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 Signature* - Firma electrónica avanzada XML)

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>

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 Factura-e 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* - Firma electrónica avanzada CMS)

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:

a. **Content-type**: esta etiqueta especifica el tipo de contenido que debe ser firmado. Es una etiqueta obligatoria según el estándar CAdES.

b. **Message-digest**: identifica el cifrado del contenido firmado OCTET STRING en encapContentInfo. Es una etiqueta obligatoria según el estándar CAdES.

c. **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.

d. **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.

e. **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.

f. **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:

b. **Content-reference**: puede ser utilizada como un modo de relacionar una
c. contestación con el mensaje original al que se refiere.
d. **Content-identifier**: esta etiqueta contiene un identificador que se puede utilizar en el atributo anterior.
e. **Commitment-type-indication**: este etiqueta indica la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...).
f. **Signer-location**: permite indicar el lugar geográfico donde se ha realizado la firma del documento.
g. **Signer-attributes**: indica el rol de la persona en la firma electrónica.
h. **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*- Firma electrónica avanzada PDF)

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 está fijado por la parte 3 del estándar PAdES "PAdES Enhanced - PAdES-BES and PAdESEPES 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 Paterna 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 Paterna 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 «Factura-e» se realizará conforme a lo regulado por la Orden PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares.

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 Paterna, 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 Paterna 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 con arreglo a la legislación:

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 Paterna

El Ayuntamiento de Paterna mantendrá actualizada en su Sede electrónica https://sedepaterna.sede.dival.es/opencms/opencms/index.html 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.

En la Política se regirá la admisión de los certificados electrónicos o digitales, a utilizar por los siguientes colectivos:

a) Certificados de los Ciudadanos/as

En función del carácter de la información a la que se accede y de las características de los servicios ofertados, y siempre conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal y al

principio de proporcionalidad recogido en la Ley 11/2007, los servicios prestados de forma electrónica, informática y telemática se clasifican de acuerdo con los siguientes **requisitos de acceso**:

- Servicios accesibles sin necesidad de identificación.
- Servicios, previa justificación, para cuyo acceso sea necesario un usuario y una contraseña numérica o alfanumérica mediante la tarjeta ciudadana del Ayuntamiento.
- Servicios de firma electrónica avanzada o reconocida.
- Servicios de difusión de información previa suscripción.

b) Certificados de la Administración Municipal

De acuerdo con el artículo 13 de la Ley 11/ 2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en relación con el artículo 3 de la Ley de Firma Electrónica 59/2003, de 19 de diciembre, la identificación del personal municipal y de los órganos administrativos se hará mediante firma electrónica avanzada basada en certificados de firma reconocidos.

El Ayuntamiento facilitará al personal municipal y a los altos cargos, un certificado electrónico que identificará de forma conjunta al titular del puesto o cargo y al Órgano en la que presta servicios.

Los órganos administrativos utilizarán sellos electrónicos que identificarán al órgano que tenga atribuida la competencia.

En los sistemas automatizados que no precisan intervención personal y directa del titular del órgano administrativo, se utilizarán certificados electrónicos que deberán incluir información sobre la identificación del órgano responsable del trámite.

Se entiende por "actuación administrativa automatizada", según la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, la actuación realizada por un sistema informático, adecuada y correctamente programado, sin que sea necesaria la intervención de una persona física.

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 (FNMT)

En el ámbito de la Administración pública:

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

  El Ayuntamiento de Paterna puede utilizar este tipo de certificados emitidos por la FNMyT-RCM para empleados públicos.

  Sus políticas y prácticas de certificación asociados están publicadas por la FNMyT-RCM en
  https://www.sede.fnmt.gob.es/certificados/administracion-publica/tipos-certificados-ap

- **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 está subordinada a la AC Raíz FNMTRCM.

Se generan en tarjeta criptográfica y tienen una longitud de clave de 2048 bits, siendo su caducidad de 48 meses

4.1.1.3 Autoritat de Certificació de la Comunitat Valenciana (ACCV)

a) Ciudadanos/as

Los certificados reconocidos de ciudadano emitidos por la ACCV se pueden utilizar para:

- Firmar y cifrar de forma segura cualquier tipo de documento electrónico incluidos los mensajes de correo electrónico.
- La identificación de usuarios ante servicios telemáticos de la Administración Pública y las entidades privadas.

b) Administración pública

- **Certificados reconocidos de empleado público**, para empleados públicos que trabajen para cualquier tipo de Administración Pública (europea, estatal, autonómica y local) así como los empleados de sus entes instrumentales, y los empleados de las Corporaciones y Universidades Públicas, que cuenten con los mecanismos de identificación requeridos (DNI, NIE, Pasaporte español), y sean empleados estas organizaciones.

- **Certificados Reconocidos de Sede Electrónica**, que sirven para identificar un portal web y establecer comunicaciones seguras, de tal forma que se garantiza la privacidad e integridad de la información que se ofrece, excluyendo la posibilidad de ser víctimas de un fraude. Básicamente es un certificado de servidor web seguro que incluye la

identificación del titular de la Sede Electrónica, y que se emite en un dispositivo seguro o medio equivalente.
La ACCV emite dos tipos de certificado de sede electrónica, en función de los dos tipos posibles de soporte, que puede ser en módulo hardware de seguridad (HSM) y en soporte software.

- **Sello de Órgano (Sellos electrónicos de Administración Pública)**, que podrá utilizarse para identificar y firmar actos administrativos por medio de sistemas informáticos sin intervención directa de la persona física competente.

  El desarrollo de la informática y de los sistemas de información ha posibilitado el concepto de actuación automatizada de las Administraciones Públicas, que puede entenderse como la producción de actos administrativos (de trámite o resolutorios) mediante sistemas de información adecuadamente programados y sin la intervención directa en el acto concreto de una persona humana.

  Estos actos automatizados siguen siendo responsabilidad de un determinado órgano administrativo y deben sustentarse en un procedimiento concreto y conocido. Como ejemplo de este tipo de actuaciones administrativas automatizadas se pueden citar el caso del registro electrónico de entrada y salida de escritos, solicitudes y comunicaciones: la presentación de documentos en el registro telemático puede hacerse a cualquier hora del día y el sistema de información devuelve el documento o parte de éste con el "recibo de presentación".

  Otros ejemplos son los certificados administrativos (certificados de empadronamiento, certificados de pago, certificado de estar al corriente con las obligaciones tributarias...), firma de Boletines Oficiales, digitalización de documentos, expedición de copias auténticas de documentos electrónicos.

  Este tipo de firmas electrónicas se denominan ***Sellos electrónicos de Administración Pública*** y se basan en un certificado digital que deberá incluir:

  - **Número de identificación fiscal (de la Administración firmante).**
  - **Denominación del órgano o Administración.**

- **Opcionalmente, la identidad de la persona titular.**

4.1.1.4 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 Paterna 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. Validación de documentos con firma digital: http://www.paterna.es/sede-electronica/es/validacion-documentos-electronicos.html

El Ayuntamiento de Paterna 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 Paterna 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 certificatevalues 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 Paterna 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 ajustará 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 Paterna, mantendrá actualizada en su Sede electrónica https://sedepaterna.sede.dival.es/opencms/opencms/index.html la relación de formatos de ficheros y objetos binarios admitidos para cada servicio, así como las limitaciones técnicas o de tamaño que puedan aplicar."

Lo que se publica, en cumplimiento de lo acordado, a los efectos oportunos.

EL ALCALDE,
Fdo.: Juan Antonio Sagredo Marco