MUNICIPIOS

Ayuntamiento de Tavernes de la Valldigna

2024/05457 *Anuncio del Ayuntamiento de Tavernes de la Valldigna sobre la aprobación definitiva del reglamento regulador de la política de firma electrónica y de certificados.*

ANUNCIO

Transcurrido el plazo de exposición pública del acuerdo adoptado por el Ayuntamiento en Pleno, en sesión ordinaria del día 12 de febrero de 2024, sobre la aprobación inicial de la modificación del Reglamento de Política de Firma Electrónica, insertado en el tablón de anuncios de esta Corporación, previo el correspondiente anuncio en el Boletín Oficial de la Provincia de Valencia n.º 39 de 23 de febrero de 2024, y dado que no se han presentado reclamaciones ni alegaciones a dicho acuerdo, de conformidad con lo previsto en los artículos 49 y 70.2 de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, y 56 del Real Decreto 781/1986, de 18 de abril,Texto Refundido de Régimen Local, queda elevado el acuerdo a la condición de definitivo con el siguiente texto íntegro:

VER ANEXO

Contra la aprobación definitiva del presente acuerdo, los interesados podrán formular directamente, en el plazo de dos meses a contar desde el día siguiente al de la publicación de la aprobación definitiva, recurso contencioso administrativo ante el Tribunal Superior de Justicia de la Comunidad Valenciana.

Tavernes de la Valldigna, a 24 de abril de 2024. —El concejal, Juan Bautista Talens Felis.

MODIFICACIÓN DEL REGLAMENTO DE POLÍTICA DE FIRMA ELECTRÓNICA Y CERTIFICADOS DEL AYUNTAMIENTO (Exp. 1635130P, referencia interna 003230024)

ELI: es-vc-01462384/reg/2024/02/__/(1)/con/202402__/spa

Preámbulo

Este documento actualiza la política de firma electrónica y certificados (PFEC) del Ayuntamiento, de acuerdo con artículo 43.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y el punto 5.7.3 del anexo del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

La PFEC del Ayuntamiento se actualiza por la necesidad de adaptarla a las modificaciones del marco regulatorio y, especialmente, por el uso de la plataforma que en cada momento se habilite como herramienta transversal de tramitación y firma, de acuerdo con el bloque normativo regulador de la identificación y firma electrónica, especialmente respecto al sistema de firma de infraestructura de clave pública, y la Resolución de 27 de octubre de 2016, de la Secretaria de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.

En consecuencia, se propone la derogación de la versión anterior i la aprobación de la nova PFEC del Ayuntamiento.

Artículo 1. Definición del alcance y ámbito de aplicación

El presente documento tiene por objeto la definición de los diferentes mecanismos de identificación y firma admitidos en la plataforma de administración electrónica del Ayuntamiento, constituida per la sede electrónica y sedes asociadas como frontal de relación con la ciudadanía, y por el conjunto de aplicaciones informáticas de tramitación de gestión como entorno de producción de la actuación administrativa municipal. La plataforma se configura distinguiendo un sistema transversal que da soporte a la gestión de todo el ciclo general de tramitación de actuaciones y expedientes, incluyendo el archivo. Junto a este sistema, se articulan subsistemas de gestión especializada que deben integrarse con el principal, en los elementos básicos de registro general de entrada, portafirmas, libro de resoluciones y actas, comunicaciones externas y archivo de oficina.

De esta manera se pretende establecer el esquema de referencia de la organización para la identificación, la autenticación y el reconocimiento de firmas electrónicas, tanto las basadas en certificados, como todas aquellas otras dentro del contexto establecido por el bloque normativo regulador de la identificación y firma electrónicas.

El ámbito de aplicación de la presente política será el de las firmas electrónicas realizadas por la organización, que afectaran a:

- Las relaciones de la ciudadanía con la organización.

- Las relaciones de la organización con otras administraciones.

Artículo 2. Adhesión a la Política de Firma Electrónica i Certificados de la Administración General del Estado

2.1 En el ámbito del sistema de firma basado en certificados, con la finalidad de posibilitar la interoperabilidad de la firma electrónica, será aplicable en este Ayuntamiento la Política de Firma Electrónica y Certificados de la Administración General del Estado, aprobada por acuerdo del Consejo Superior de Administración Electrónica, en reunión de la Comisión Permanente de 30 de mayo de 2012, y publicada en el BOE núm. 299, de 13 de diciembre de 2013, así como sus revisiones o versiones que en el futuro se produzcan, además de las políticas específicas de los prestadores cualificados de servicios de confianza en la medida en que resulten aplicables de acuerdo con la normativa europea reguladora de la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, sin necesidad de adoptar un nuevo acuerdo.

2.2 Asimismo, a fin de regular las peculiaridades derivadas de la naturaleza de administración local de este Ayuntamiento, serán aplicables, además, las normas que se establecen en los siguientes preceptos.

Artículo 3. Datos para la identificación del documento y del responsable de su gestión

El presente documento de política de firma electrónica y de certificados tendrá un identificador único, y se asignarán los dos últimos dígitos a la versión que corresponda, a fin de distinguir las versiones sucesivas que puedan existir cuando se realicen actualizaciones.

En el caso de que se trate de una firma electrónica basada en certificado, la identificación de la política de firma aplicable, consignada en las propiedades firmadas de la firma, será la versión vigente emitida por la Administración General del Estado, a la que este Ayuntamiento se ha adherido. No obstante, explícitamente se aplicarán a esta firma aquellas condiciones adicionales derivadas del ámbito de competencia municipal referidas en este documento.

La presente política de firma electrónica y de certificados será válida desde la fecha de emisión indicada hasta que sea derogada o se publique una nueva versión. Los períodos de transición serán indicados en las nuevas versiones y, una vez transcurridos los plazos indicados, serán válidas únicamente las versiones actualizadas.

Además, en el caso de actualización de la presente política de firma electrónica y de certificados, se identificará el enlace URL donde encontrar las versiones anteriores para verificar una firma electrónica anterior a la política vigente.

Identificador de la política	
Nombre del documento	Política de firma electrònica y de certificados del Ayuntamiento de Tavernes de la Valldigna
Versión	2.0
Identificación del documento	https://www.tavernes.es/va/transparencia/reglament-politica-signatura-electronica-certificats-lajuntament
URL de referencia	https://www.tavernes.es/va/transparencia/normativa-municipal
Fecha de emisión	12/02/2023
Àmbito de aplicación	Ajuntament de Tavernes de la Valldigna - DIR3 L01462384

Al gestor de la presente política de firma electrónica y de certificados le corresponde el mantenimiento, actualización y publicación electrónica de los criterios sobre firma electrónica.

Identificador del gestor	
Nombre del gestor de la política	Departament d'Informàtica de l'Ajuntament de Tavernes de la Valldigna
Dirección de contacto	Plaça Major, 1 Tavernes de la Valldigna (València, España) 46760

Artículo 4. Reglas comunes para el firmante, el creador del sello, y el verificador de la firma o sello electrónicos

4.1 Las reglas comunes establecen las responsabilidades respecto a la firma electrónica sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definen los requisitos mínimos que han de presentarse, y en el ámbito del sistema de firma basada en certificados, deberán estar firmados si son requisitos para el firmante, o no firmados si son requisitos para el verificador.

Estas reglas se definen de acuerdo con los sistemas y formatos de firma electrónica admitidos, teniendo en cuenta los diferentes usos de la firma electrónica, el uso de algoritmos y los procesos de creación y validación de firma.

4.2 Reglas del firmante

El firmante será responsable de que el fichero que se quiere firmar no incorpora contenido dinámico que pudiera 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 de que no existe contenido dinámico dentro del fichero, como pueden ser macros, todo ello de acuerdo con lo que se indica en el anexo 1 de la presente Política.

4.3 Reglas del verificador

El encargado de la verificación de la firma será responsable de definir los procesos de validación y de archivado, de conformidad con los requisitos de la política de firma particular a la que se ajusta el Servicio y con lo establecido en la NTI de política de gestión de documentos electrónicos, de acuerdo con lo en el anexo 2 de la presente Política.

Artículo 5. Reglas de confianza

5.1 Reglas de confianza de certificados electrónicos.

Para ejecutar la firma electrónica de contenido se consideran válidos aquellos certificados reconocidos de conformidad con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y con el Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (ReIDAS) y los sistemas de firma y certificados electrónicos de acuerdo con el artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En consecuencia, los certificados admitidos son los que siguen:

a) Sistemas de firma electrónica cualificada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores cualificados de servicios electrónicos de confianza".

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico incluidos en la "Lista de confianza de prestadores cualificados de servicios electrónicos de confianza".

La relación de sellos electrónicos utilizados por el Ayuntamiento de Tavernes de la Valldigna, que indica las características de los certificados electrónicos y los prestadores que los expiden, será pública y accesible a través del punto de acceso electrónico general (https://www.tavernes.es/va/transparencia/normativa-municipal).

Adicionalmente, la verificación de los sellos y certificados electrónicos, incluyendo el de la misma Sede, se podrá efectuar a través de la Aplicación de validación de firma y certificados en línea y de servicios de @firma u otros Sistemas reconocidos de validación electrónica.

5.2 Reglas de confianza para los sellos de tiempo

El sello electrónico de tiempo asegura que tanto los datos originales de lo que será 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, de acuerdo con las indicaciones del anexo 3.

5.3 Reglas de confianza para firmas longevas

La validación se hará de acuerdo con lo dispuesto en el anexo 4.

5.4 Firma biomètrica

La firma biométrica se considerará, con carácter general en el ámbito municipal y en los procedimientos habilitados, equivalente a la firma manuscrita, siempre que se realice en presencia de personal empleado público que garantizará la identidad del firmante, y siempre que se usen los dispositivos homologados por el Ayuntamiento.

Se seguirá el procedimiento descrito en el anexo 5.

5.5 Firma ocultando los datos personales del firmante

En el ámbito de la presente política, una firma ocultando los datos personales del firmante consiste en una firma electrónica o biométrica cuyos datos personales no están disponibles públicamente al verificar el correspondiente CSV. En algunas aplicaciones de gestión municipal este tipo de firma se denomina "firma con seudónimo." Entre estas firmas, los datos personales se encuentran en la firma propiamente dicha si está basada en certificado. En todo caso, los datos identificativos de la persona firmante (NIF, nombre y apellidos) estarán disponibles para los administradores de las aplicaciones de gestión, en caso de ser necesario. El resto de personas únicamente podrán visualizar el seudónimo utilizado en la firma, salvo que se haya de facilitar la firma electrónica original.

Artículo 6. Reglas adicionales de creación y validación de firma para documentos electrónicos

6.1 Naturaleza y contenido

La firma electrónica corporativa deberá tener el carácter de avanzada en general y cualificada en los supuestos previstos, y habrá de cumplir, además, los siguientes requisitos:

a) Estar amparada por un certificado cualificado en todo caso, emitido por un prestador de servicios de certificación de los incluidos en la lista de confianza de prestadores cualificados a que se refiere la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

b) Vincular unos datos de verificación de firma a la identidad del titular, su condición de órgano unipersonal en ejercicio de su cargo público (alcalde o concejales delegados, secretario, interventora y tesorera) o funcionario autorizado del Ayuntamiento en servicio activo y la plaza de destino.

c) Expresar que el uso de la firma electrónica está limitado exclusivamente a la subscripción de documentos públicos u oficiales propios del oficio del signatario.

d) Corresponderse con un dispositivo seguro de creación de firma, cuando se trate de un supuesto previsto de firma cualificada. El dispositivo de creación habrá de ajustarse a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

6.2 Los órganos unipersonales dispondrán de firma electrónica corporativa desde el momento de su nombramiento. De la misma manera se habrá de proceder cuando se produzca la revocación o expiración del período de validez del certificado precedente.

6.3 El secretario y otros habilitados nacionales del Ayuntamiento, así como otro personal que necesite firma corporativa, habrán de obtener, en el momento de la toma de posesión, una firma electrónica. De la misma manera se habrá de proceder cuando se produzca la revocación o expiración del período de validez del certificado precedente.

En el caso de los empleados públicos que por razón de sus funciones o bien por la temporalidad de su prestación de servicio, así esté previsto, podrán hacer uso de su certificado personal siempre que:

a) Sea un certificado que cumpla las condiciones de artículo 6.1.a) y esté vigente.r

b) Disponga de una cuenta de usuario, expresamente comunicada por el Departamento de Informática, en la aplicación informática en la que use dicho certificado.

c) El certificado se usará básicamente para identificación en sistemas informáticos, pero no para firmar documentos administrativos. Excepcionalmente, para documentos de ámbito interno, podrá usar el certificado personal para la firma, pero siempre dentro de la aplicación informática de gestión correspondiente, consignando en las propiedades firmadas el identificador de la política de firma del Ayuntamiento.

6.4 En el momento que el Departamento de Recursos Humanos comunique al Departamento de Informática la incorporación de la persona al puesto de trabajo, se habrán de generar los datos de creación de firma por parte del Departamento de Informática, con intervención personal del firmante, salvo que se trate de un supuesto de empleado público temporal referido en el apartado anterior. En este caso, será el usuario quien hará la instalación del certificado personal en el repositorio de la aplicación correspondiente que autorice el Departamento de Informática. Una vez el empleado finalice su prestación de servicios con el Ayuntamiento, habrá de desinstalar el certificado el último día de prestación del servicio.

Los prestadores de servicios de certificación en ningún caso podrán almacenar ni copiar los datos de creación de firma.

6.5 Los prestadores de servicios de certificación no podrán emitir los certificados que amparen las firmas electrónicas profesionales del personal del Ayuntamiento hasta que hayan recibido notificación electrónica, firmada por el alcalde o concejal delegado

competente, expresiva de los datos de verificación de firma del firmante y acreditativa de la condición de órgano unipersonal, secretario y otros habilitados nacionales del Ayuntamiento, así como otro personal que necesite firma corporativa, de su situación de servicio activo, de su plaza de destino y de haberse cumplido los requisitos de asunción de la firma electrónica establecidos en este documento.

En caso de que se arbitre una fórmula jurídica para que el Ayuntamiento funcione como punto de registro unificado de un prestador de servicios cualificado, para la generación/revocación de certificados de empleado público, se usará la plataforma que dicho prestador establezca. En este caso el Departamento de Informática generará/revocará los mencionados certificados directamente, siguiendo las instrucciones técnicas y operativas establecidas por el citado prestador.

6.6 Todos los titulares de firma electrónica corporativa estarán obligados a custodiar personalmente, adoptando las medidas de seguridad adecuadas, los datos de creación de firma electrónica que les corresponda. El titular, bajo su responsabilidad, no cederá su uso a ninguna otra persona. Habrá de denunciar inmediatamente al alcalde o presidente su pérdida, extravío o deterioro, así como cualquier situación o caso que pueda poner en peligro el secreto o la integridad del mecanismo. Ante esta situación, inmediatamente se comunicará al prestador de servicios de certificación que haya expedido el certificado o a quien le haya sido transferido, para que inmediatamente lo suspenda o revoque.

En especial, aquellos usuarios que dispongan de un certificado diferente del de empleado público instalado en el ordenador asociado al puesto de trabajo, han de velar para que su uso solo se haga de acuerdo con las instrucciones recibidas y siempre bajo los requerimientos mínimos de seguridad aprobados por el Ayuntamiento. Una vez finalizada su relación de servicios con el Ayuntamiento habrán de desinstalar dicho certificado el último día de prestación de servicios.

6.7 En todo caso, los prestadores de servicios de certificación habrán de revocar inmediatamente sus certificados a instancia del alcalde o presidente de la corporación, que habrá de ordenarlo a solicitud del firmante conforme al párrafo anterior, y cuando se produzca su cese en el puesto de trabajo. En los supuestos de interrupción temporal de las funciones del firmante previstos en la legislación aplicable, o a requerimiento de él, se suspenderá si es posible o se revocará, en su caso, el certificado correspondiente.

6.8 El Ayuntamiento, a través de sus medios correspondientes, habrá de garantizar a los prestadores de servicio de certificación que lo soliciten, la condición de órgano unipersonal o empleado público en activo en el momento de la firma del documento, la vigencia, revocación y suspensión del certificado electrónico, mediante el mantenimiento de un directorio actualizado de certificados debidamente protegido, así como un servicio de consulta permanente, rápido y seguro.

6.9 Asimismo, se habrá de aplicar el mecanismo de sellado de tiempo de los documentos firmados electrónicamente que se detallan en esta PFEC. Con esta finalidad, han de disponer de sistemas horarios homogéneos que han de sincronizar

sus respectivos sistemas de sellado de tiempo con la señal horaria del Real Instituto y Observatorio de la Armada, de conformidad con el Real Decreto 1308/1992, de 23 de octubre, por el que se atribuye a ese laboratorio la función de depositario del Patrón Nacional de Tiempo.

6.10 En todo caso, el Ayuntamiento habrá de establecer una sola fuente de sellado de tiempo sincronizada en los términos expuestos en el párrafo precedente para todos los documentos.

6.11 Corresponde a la Alcaldía o Presidencia la inspección y control del cumplimiento de lo previsto en este apartado y, especialmente, lo relativo al examen y verificación técnica de los requisitos que han de cumplir las diferentes redes telemáticas, sistemas de acreditación y verificación de la vigencia de los certificados electrónicos y sistemas de sellado de tiempo.

En el ejercicio de esta competencia podrá requerir la colaboración de los órganos técnicos que considere oportuno, así como ordenar mediante instrucciones a las diferentes unidades organizativas que adopten las medidas necesarias para el funcionamiento del sistema.

6.12 Se llevará un registro de los certificados electrónicos corporativos, así como de los certificados personales que se usen para la identificación del empleado público en las funciones a desplegar, mientras sea titular del correspondiente puesto de trabajo en el Ayuntamiento, a los efectos de su gestión y auditoria.

6.13 El Departamento de Informática será encargado, en exclusiva, de verificar que los certificados siempre estén instalados con nivel de Seguridad alta, que requiere la introducción de una contraseña para hacer uso del mismo.

Artículo 7. Sellos de administración y de órgano

7.1 De acuerdo con la Ley 40/2015, se autoriza el uso del sello electrónico de administración y de órgano del Ayuntamiento para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada. El certificado electrónico del sello electrónico de órgano del Ayuntamiento incluirá la denominación correspondiente y el NIF del Ayuntamiento.

7.2 La relación de sellos electrónicos utilizados por el Ayuntamiento, incluyendo las características de los certificados electrónicos y los prestadores que los expiden habrá de ser pública y accesible por medios electrónicos en el punto de acceso electrónico general (https://www.tavernes.es/va/transparencia/normativa-municipal.). Además, se adoptarán les medidas adecuadas para facilitar la verificación de los sellos electrónicos.

7.3. El sello electrónico de administración se podrá utilizar para migraciones y cambios de formato automáticos, en particular a los efectos de archivo, así como para el

intercambio automático de datos entre administraciones en entornos cerrados y abiertos.

7.4. El sello electrónico de órgano se podrá utilizar para la firma de actuaciones administrativas automatizadas, en los términos del art. 42 de la Ley 40/2015.

Artículo 8. Identificación y firma electrónica

Dentro del marco establecido por el marco normativo que regula la identificación y firma electrónica, el Ayuntamiento, en función del tipo de procedimiento y su regulación previa, respecto a este apartado, reconoce:

8.1. Firma basada en identificación más voluntad de firma (sistema de claves concertadas). En especial se reconoce el sistema regulado en la Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve.

Asimismo, también se admite el sistema de identificación soportado por la misma plataforma Cl@ve.

En el caso de los empleados públicos que por razón de sus funciones o bien por la temporalidad de su prestación de servicio así esté previsto, podrán hacer uso de su identificación personal en Cl@ve, siempre que:

a) Disponga de una cuenta de usuario, expresamente comunicada por el Departamento de Informática, en la aplicación informática en la que esté habilitado el uso de dicha identificación.

b) Esta identificación no se usará para la firma, salvo que sea para actuaciones de ámbito interno y siempre que fuera posible dentro de la aplicación informática de gestión correspondiente.

8.2. Firma manuscrita sobre tableta electrónica.

8.3 Firma basada en Código Seguro de Verificación.

8.4 En función de la categoría de los Sistemas de información conforme al Esquema Nacional de Seguridad, para los documentos producidos mediante Actuaciones Administrativas Automatizadas se podrà habilitar como sistema de firma un sistema CSV.

8.5 La aprobación del uso de este sistema de firma se hará en la resolución que regule la Actuación Administrativa Automatizada, previo análisis de los requerimientos tecnológicos, jurídicos y de gestión documental, de acuerdo con las previsiones del ENS.

8.6 Otros Sistemas de identificación y firma que el Ayuntamiento reconozca prèvia regulación del procedimiento y los medios informáticos dentro de los que será aplicable.

Artículo 9. Seguridad

Todos los documentos del Ayuntamiento que requieran firma electrónica aplicaran las medidas de seguridad referentes a firma electrónica exigibles en el nivel medio, y las de nivel alto en los términos y con las condiciones establecidas en el Esquema Nacional de Seguridad.

Artículo 10. Gestión de la política de firmas

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al área de Informática del Ayuntamiento, que mantendrá tanto la versión actualizada del presente documento como un repositorio con el historial de las versiones anteriores.

En 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 (punto de acceso electrónico general https://www.tavernes.es/va/transparencia/normativa-municipal).

10.1 Archivo y custodia

Las transmisiones de datos firmadas se almacenarán el tiempo que resulte imprescindible para la acreditación de su validez a largo plazo.

El contenido firmado en el sistema basado en certificado, para garantizar la fiabilidad de una firma electrónica y que ésta tenga efectos jurídicos frente a terceros a lo largo del tiempo, habrá de ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo, así como los certificados que conformen la cadena de confianza incorporando sellos de tiempo para los elementos añadidos. Toda esta información se almacenará en un repositorio de no repudio, entendido como un concepto vinculado a las prevenciones que han de observar las aplicaciones de gestión municipal que capturen documentos externos firmados o que generen firmas electrónicas.

Con la vocación de configurar un archivo único municipal para la conservación a lo largo del tiempo de documentos e índices de expediente y sus firmes, bajo los requisitos de autenticidad, integridad y no repudio, las aplicaciones informáticas de gestión observaran los requisitos siguientes:

a) En el sistema se almacenarán todas las firmas del contenido, tanto las realizadas con certificado de persona física o jurídica como con sello de órgano o equivalente, ya hayan sido realizadas internamente en el ámbito de les aplicaciones del organismo (se

almacenarán en el momento de su creación) como en el exterior (se almacenarán en el momento de la su validación).

b) En cualquiera de los casos, se almacenará como mínimo la firma y un sello de tiempo.

c) Respecto a las firmas basadas en certificados, se almacenará, como mínimo, la firma con sello de tiempo (formatos XadEST/CadES-T/PadES-EPES con atributo signature-estafe-stamp). Si se necesitara conservación a largo plazo de la firma, se almacenará en formato XAdES-A/CAdES-A/PAdES-LTV que asegura la totalidad del documento y les firmes contenidas. Se procederá al resellado de las firmas cuando proceda o sea necesario para cualesquiera otras medidas técnicas precisas.

10.2 Obsolescencia de los algoritmos

Específicamente, para proteger la firma electrónica frente a la posible obsolescencia de los algoritmos y poder continuar asegurando sus características de validez, las aplicaciones de gestión especializada transferirán documentos y expedientes a la aplicación transversal de gestión, siguiendo la Política de Gestión Documental del Ayuntamiento y sus instrucciones de desarrollo.

Mientras no se produzca dicha transferencia, por parte de las aplicaciones de gestión especializada y para garantizar la conservación a largo plazo, estas aplicaciones utilizaran mecanismos de sellado y resellado de tiempo. Una vez hecha la transferencia, será en la aplicación transversal donde se harán las operaciones de resellado.

Artículo 11. Autenticidad de los documentos

La autenticidad de las firmas electrónicas y documentos producidos en el ámbito de esta política se acreditará y verificará en las siguientes condiciones.

11.1 Código seguro de verificación (CSV)

El código seguro de verificación de un documento identifica biunívocamente a un documento y un conjunto de firmas y/o sellos electrónicos.

Su conocimiento permite el acceso en la sede electrónica o sede asociada a un documento en formato PDF. El interesado podrá obtener el sellado electrónico del documento en esta sede para garantizar la autenticidad e interoperabilidad. En el PDF mencionado se incluye el documento íntegro originalmente firmado y la correspondiente información de les firmas.

El CSV proporcionará acceso a la siguiente información:

- Documento CSV.

- Documento original.

- Firmas electrónicas en el formato en el que son producidas.

- Otra información relativa al documento firmado (identificación de las personas firmantes, fecha y hora de las firmes, título del documento, etc.).

11.2 Procedimiento de verificación de los documentos con CSV generados por la plataforma

Se garantizará que cualquiera, empleado o empleada pública de esta administración o tercera parte independiente, tenga la capacidad de comprobar, por una parte, la validez, autenticidad e integridad de los documentos con CSV generados en el ámbito de esta política y, por otra, la validez, autenticidad e integridad de la información y firmas asociadas a estas.

Para realizar la verificación se habrán de utilizar medios o dispositivos informáticos en condiciones seguras (no comprometidos o libres de programas maliciosos).

Cuando se acceda mediante un navegador web a la dirección de la Sede electrónica o sede asociada, lugar donde se podrán verificar los documentos CSV, se habrá de comprobar que no muestra ninguna alerta sobre la validez del certificado SSL.

Los diferentes procedimientos de verificación se detallan en el anexo 6.

Artículo 12. Sistemas de firma para la Actuaciones Administrativas Automatizadas.

12.1. En función de la categoría de los sistemas de información conforme al Esquema Nacional de Seguiridad, para los documentos creados mediante Actuaciones Administrativas Automatizadas, se podrá habilitar como sistema de firma un CSV de acuerdo con la normativa de aplicación.

12.2. La aprobación del uso de estos sistemas de firma se realizará en la resolución que regule la Actuación Administrativa Automatizada, con análisis previo de los requerimientos tecnológicos, jurídicos y de gestión documental, de acuerdo con las previsiones del ENS.

Disposición derogatoria

Queda derogada la Política de Firma Electrónica y Certificados de este Ayuntamiento, aprovada por Resolución de la Alcaldía-Presidencia de 7 de octubre de 2014.

ANEXOS

Los presentes anexos ofrecen indicaciones sobre las diversas operativas. Podrán ser modificados por Resolución de Alcaldía o de la concejalía delegada competente.

Anexo 1. Reglas del firmante

En casos de firma basada en certificados electrónicos:

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

a) SigningTime: indica la fecha y la hora. En el caso de firma en cliente sin acceder a servidor, será meramente indicativa (porque la fecha en el dispositivo cliente es fácilmente manipulable) y/o será utilizada con finalidades diferentes a conocer la fecha y hora de firma.

b) SigningCertificate: contiene referencias a los certificados y algoritmos de seguridad utilizados para cada certificado. Este elemento deberá ser firmado con el fin de evitar la posibilidad de sustitución del certificado.

c) SignaturePolicyIdentifier: identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica, y ha de incluir los siguientes contenidos en los elementos en que se subdivide como sigue.

- Una referencia explícita al presente documento de política de firma 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>

- 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 està generada según la misma política de firma que se utilizara para su validación.

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

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

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

- SignerRole: define el rol de la persona en la firma electrónica. Al menos uno de estos elementos ClaimedRoles o CertifiedRoles han de estar presentes en este campo: "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 diferente del emisor o del receptor.

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

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

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

Anexo 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 que se ha generado la firma, independientemente del formato utilizado (XAdES, CAdES o PAdES), son los siguientes:

a) 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.

b) Signing Certificat: 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 de 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 prestador de servicios de certificación (PSC) ofrezca un servicio de validación histórico del estado del certificado.

c) Signature Policy: se habrá de comprobar que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que se ha de utilizar para un servicio en cuestión.

Existe un tiempo de espera, conocido como período de precaución o período de gracia, para comprovar el estado de revocación de un certificado.

El encargado de la verificación podrá esperar este plazo para validar la firma o realizarla en el mismo momento y revalidarla después.

El período desde que se realiza la firma o el sellado de tiempo deberá abarcar, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs o el tiempo máximo de actualización del estado del certificado en el servicio OCSP. Estos plazos podrán variar en función del prestador de servicios de certificación.

Anexo 3. Reglas de confianza para los sellos de tiempo

El formato del sello de tiempo habrá de 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 són:

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

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

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

- Fecha y hora UTC.

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

El sellado de tiempo puede ser añadido por el emisor, el receptor o un tercero y se ha de incluir como propiedad no firmada en el campo Signature Time Stamp. El sellado de tiempo ha de 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 per prestadores de servicios de sello de tiempo que cumplan las especificaciones técnicas ETSI TS 102 023, "Electronic Signatures and Infrastructures (ESI); Policy requirements for estafe-stamping authorities".

Anexo 4. Reglas de confianza para firmas longevas

Los estàndardes XAdES (ETSI TS 101 903) en sus diferentes versiones 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 período de validez del certificado. La información podrá ser incluida por el firmante o por el verificador, habrá de hacerse transcurrido el período de precaución o 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 éstos.

- Los certificados que conformen la cadena de confianza.

En el caso de que se desee generar firmas longevas, se habrá de incluir la información de validación anterior, y añadirle un sello de tiempo.

En este tipo de firma la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva. En el caso de que se desee incorporar a la firma la información de validación, se habrá de usar validación mediante OCSP (Online Certificadoe Estatus Protocol), 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 generara un elevado volumen de información, alternativamente a la información de validación indicada anteriormente, se podrá incluir en la firma longeva referencias a esta información. 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 de los certificados.

En el caso de que se desee incorporar a la firma la información de validación, se utilizará 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, adicionalmente a las referencias a la información de validación, 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 de que es 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.

Anexo 5. Firma biométrica

Se seguirá el siguiente procedimiento:

a) El personal empleado público solicita el DNI a la persona firmante y comprueba que sus datos identificativos se corresponden con los que consten en el sistema.

b) El sistema compone el documento de firma combinado:

b.1) Se eliminan los espacio en blanco, y se obtiene su forma canónica según el procedimiento estàndard del W3C (https://www.w3.org/tr/xmlc14n11/).

b.2) Se calcula el hash SHA3-512.

c) Se informa a la persona firmante sobre los datos a firmar:

c.1) Por una parte, se muestra en la pantalla del dispositivo de firma tanto el hash calculado como la fecha y hora del PC al que está conectado.

c.2) De otra parte, este mismo hash y la correspondiente relación de documentos PDF a firmar se pondrán a disposición de la persona firmante a través de una pantalla de visualización, para su cotejo, antes de solicitarle que firme.

d) La persona firmante realiza la firma.

e) El personal empleado público comprueba que la firma trazada corresponde con la firma que consta en el DNI i la acepta.

e) El sistema almacena el fichero de firma generado por el dispositivo y el dibujo de la firma.

f) El sistema sella electrónicamente el documento XML correspondiente a la firma biométrica, con el hash mostrado en la pantalla del dispositivo antes de firmar y el contenido del fichero de firma generado, así como los datos personales de la persona firmante y los datos personales del personal empleado que recoge la firma.

Por motivos de seguridad de la información y protección de los datos de carácter personal, ni la firma biométrica ni el sello de tiempo serán accesibles públicamente mediante el CSV. Sí que lo será el trazo de la firma, igual que sería visible la rúbrica de la firma manuscrita en un documento en papel.

Los administradores de la Sede podrán acceder a la información de forma completa en caso de que fuera necesario.

Anexo 6. Procedimiento de verificación de los documentos con CSV generados por la plataforma

1 Verificación de documentos con CSV emitidos en papel

Una vez se esté en posesión del documento en papel con CSV se seguirán los siguientes para su verificación:

a) Acceder mediante el sistema de identificación requerido en la sede electrónica o sede electrónica asociada y un navegador web a la dirección de verificación de CSV de la sede electrónica (asimismo reflejada en el propio documento).

b) Introducir el código CSV impreso en el margen del documento.

c) Comprobar que la sede electrónica indica que existe un documento con este CSV y que al descargarlo coincide con el documento impreso (han de ser idénticos).

2 Verificación de documentos con CSV emitidos en formato electrónico (PDF)

Una vez se esté en posesión del documento electrónico con CSV se seguirán los siguientes pasos para su verificación:

a) Validar las firmas del documento CSV mediante la aplicación Valide de la Administración General del Estado o mediante un programa lector de documentos PDF con la capacidad de verificar firmas electrónicas en formaot PAdES LTA-level:

a.1) Si el CSV consta de 20 dígitos: comprobar que la aplicación acredita que la firma es válida y que el documento está firmado mediante un certificado de sello electrónico incluido en el listado al que se hace referencia en el artículo 7 de la presente política. Si la firma contiene sello de tiempo, este también ha de presentarse como válido (PAdES LTA-level).

a.2) Si el CSV consta de menos de 20 dígitos: comprobar que la aplicación acredita que las firmas son válidas. Si la firma contiene sello de tiempo, este también ha de presentarse como válido.

b) Adicionalmente, comprobar que el documento CSV existe en la sede electrónica:

b.1) Acceder mediante un navegador web a la dirección de verificación de CSV de la sede electrónica (asimismo reflejada en el propio documento).

b.2) Introducir el código CSV impreso en el margen del documento.

b.3) Comprobar que la sede electrónica indica que existe un documento con este CSV y que al descargarlo coincide con el documento electrónico (han de ser idénticos).

3 Verificación de documentos de firma electrónica XAdES

Los documentos de firma XAdES producidos en el ámbito de esta política estarán asociados a sus correspondientes documentos originales o a sus correspondientes documentos CSV.

La autenticidad y validez de las firmas electrónicas XAdES se acreditará y verificará siguiendo el siguiente procedimiento:

a) Recabar la siguiente información:

- Documento original.

- Fichero de firma electrónica en formato XAdES-A.

- Título del documento.

- Información de la persona firmante.

- Código aleatorio (salt o sal) con el que se generó la huella firmada en el documento XAdES-A.

b) Validar el fichero de firma electrónica mediante la aplicación Valide de la Administración General del Estado. Al ser un formato estándar, se pueden usar otras herramientas con capacidad de validación de firmas.

c) Comprobar que la firma validada en el punto anterior se corresponde con el documento firmado:

c.1) Calcular el hash SHA3-512 sobre el resultado de concatenar el documento binario original + el título del documento codificado en UTF-8 + la información del firmante codificada en UTF-8 + la "sal".

c.2) Abrir el fichero XAdES-A y comprobar que el elemento en la ruta XPath /ds:Signature/ds:Object/documentos_signats contiene un elemento documento_firmado con el hash calculado anteriormente y la "sal" utilizada (ambos codificados en Base64).

c.3) Comprobar que el XPath anterior se encuentra incluido en alguna de las referencias del elemento SignedDataObjectProperties, y por tanto, firmado.

En caso de que todas las comprobaciones anteriores hayan resultado satisfactorias, quedaría probado que el documento original se corresponde con la firma XAdES-A, que garantiza la integridad del documento, su autenticidad y el no repudio.

Dado que la validación de la firma XAdES resulta un procedimiento complejo, se publicará una herramienta que de forma automática permita verificar su correspondencia con el documento original firmado.

Adicionalmente, el codigo fuente de esta herramienta se publicará sin restricciones de acceso en un repositorio a este efecto. De esta manera los terceros que dispongan de los medios y conocimientos tecnológicos precisos podrán generar la herramienta que les permita verificar de forma autónoma e independiente la validez de los documentos producidos en el ámbito de esta política.