EUSKO JAURLARITZA GOBIERNO VASCO

HERRI ADMINISTRAZIO ETA JUSTIZIA SAILA

DEPARTAMENTO DE ADMINISTRACIÓN PÚBLICA Y JUSTICIA

Política de firma electrónica basada en certificados de la Administración Pública de la Comunidad Autónoma de Euskadi

Donostia - San Sebastián, 1 – 01010 VITORIA-GASTEIZ
tef. 945 01 85 71 – Fax 945 01 87 01

Contenido

Capítulo/sección *Página*

1. Introducción

El Decreto 21/2012, de 21 de febrero, de Administración Electrónica tiene el objetivo de desarrollar, en el ámbito de la Administración Pública de la Comunidad Autónoma de Euskadi, el derecho de la ciudadanía a relacionarse con la Administración, por medios electrónicos, para acceder a los servicios públicos y para la tramitación de los procedimientos administrativos.

A un nivel general, el Decreto regula aspectos tales como la sede electrónica, el tablón electrónico de anuncios, la identificación y autenticación, los registros electrónicos, las comunicaciones y notificaciones, los documentos electrónicos y sus copias, la tramitación electrónica o los servicios electrónicos comunes.

Más concretamente, en el artículo denominado "*Política de firma y de certificados*", correspondiente al título de identificación y autenticación, se establece que la Administración aprobará y publicará su política de firma electrónica y de certificados, y que ésta concretará los procesos relativos a la generación, validación y conservación de firmas electrónicas, así como otros requisitos exigibles a las mismas. Asimismo, establece que ésta se publicará por Orden del Departamento competente en Administración Electrónica.

La Orden por la que se aprueba la política de firma electrónica y de certificados es el instrumento por el cual se procede a la publicación y difusión pública de la misma.

Este documento amplía lo especificado en la Orden por la que se aprueba la política de firma electrónica y de certificados y presenta una estructura normalizada del documento electrónico en relación con la creación y validación de firma electrónica, según los estándares técnicos europeos, para facilitar la interoperabilidad de estos documentos, describiendo el alcance y uso de la firma electrónica con la intención de cumplir las condiciones para una transacción concreta en el contexto de la Administración Pública de la Comunidad Autónoma de Euskadi, en adelante CAE.

2. Alcance de la política de firma

Este documento propone una política de firma electrónica, que detalla las condiciones generales para la generación, validación y conservación de la firma electrónica y una relación de formatos de objetos binarios y ficheros de referencia que deberán ser admitidos por todas las plataformas implicadas en las relaciones electrónicas de la Administración con la ciudadanía y sus Organismos Autónomos, Entes Públicos de Derecho Privado y demás entidades incluidas en el ámbito de aplicación del Decreto de Administración Electrónica.

Para su identificación unívoca, la presente política de firma se identificará con un identificador único en forma de URI, que deberá incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente para identificar la política de firma y la versión con las condiciones generales y específicas de aplicación para su validación, determinando las condiciones que debe cumplir la firma electrónica en un momento determinado.

La presente política de firma estará disponible en formato legible, de modo que puedan ser aplicadas en un contexto concreto para cumplir con los requerimientos de creación y validación de firma electrónica.

2.1. Actores involucrados en la firma electrónica

Los actores involucrados en el proceso de creación y validación de 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 una política de firma concreta. Puede 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 firma electrónica: la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

- Emisor 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 y el verificador en los procesos de generación y validación de firma electrónica.

2.2. Formatos admitidos de firma

El formato de los documentos electrónicos con firma electrónica avanzada y reconocida, aplicada mediante los certificados electrónicos admitidos por la Administración y utilizados en el ámbito de las relaciones con o dentro de la Administración se deberá ajustar a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica y a la legislación española en el caso de firma electrónica reconocida.

La Dirección competente en Administración Electrónica será la encargada de publicar y actualizar, en la sede electrónica, la relación de las especificaciones relativas a los formatos admitidos por la presente política de firma.

La Dirección competente en Administración Electrónica conservará un repositorio con el historial de las versiones de la política de firma electrónica y de certificados que se aprueben. La consulta a este repositorio permitirá verificar una firma electrónica anterior a la política vigente en cada momento. En el momento de la firma, se deberá incluir la referencia del identificador de la versión de la política de firma electrónica y de certificados que determinará las condiciones que debe cumplir la firma electrónica en cada momento.

Se tendrá en cuenta la legislación Europea en relación a los formatos de firma admitidos en la Unión Europea, en especial, aquellos definidos en los estándares europeos de firma electrónica.

Dentro de las distintas clases del formato XAdES, los órganos y organismos incluidos en el ámbito de aplicación del Decreto de Administración Electrónica, deberán adecuar sus sistemas para la generación de, al menos, la clase básica, añadiendo información sobre la política de firma (clase EPES), y la verificación de las diferentes clases del formato XADES versión 1.3.2, según se recoge en la especificación técnica ETSI TS 101 903.

La clase básica de firma electrónica para definir una política de firma electrónica de interoperabilidad es según los estándares AdES la clase EPES. A partir de este formato básico EPES es posible incluir suficiente información para validar la firma a largo plazo.

Para la validación a largo plazo, se utilizará un formato XAdES- A que incorpore la posibilidad de timestamping periódico sobre las propiedades adicionales, como información sobre las referencias a los certificados y valores de revocación, además de los propios certificados y valores de revocación obtenidos de las listas de revocación CRLs o servicios OCSPs.

2.2.1. Firma electrónica de transmisiones de datos

Tal y como establece el Esquema Nacional de Interoperabilidad, en adelante ENI, la firma electrónica de transmisiones de datos estará basada en los estándares recogidos en la *Norma técnica de Interoperabilidad de Catálogo de estándares*.

En el caso particular de esta política de firma, la transmisión de datos está basada en servicios Web. Por tanto, será de carácter obligatorio la aplicación de firmas electrónicas según el estándar *WS- Security: SOAP Message Security* de OASIS, en particular, con la especificación estándar *X.509 Certificate Token Profile*.

2.2.2. Firma electrónica de contenido

En la política de firma se deberá especificar los formatos admitidos para la firma de contenido. Atendiendo a la *Norma técnica de Interoperabilidad de Catálogo de estándares* y a las características particulares de esta política de firma, el formato que se acepta es el siguiente:

a. XAdES (XML Advanced Electronic Signature), según la especificación técnica ETSI TS 101 903, versión 1.3.2.

A su vez, este formato podrá tener las siguientes variantes:

- ✓ -*T*: formato mínimo para el cumplimiento de la política de firma del Gobierno Vasco. Se ha añadido un campo de sellado de tiempo para proteger contra el no repudio.
- ✓ -A: incluye un sello de tiempo periódico sobre las referencias a los certificados y listas de revocación, además de los propios certificados y listas de revocación. De esta forma, se consiguen firmas longevas que perduran durante largos periodos de tiempo.

2.3. Creación de la firma electrónica

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

1. Selección por parte del usuario firmante del fichero para ser firmado. Los formatos de fichero que deberán ser admitidos por las plataformas, están publicados en la sede electrónica, en el apartado documentos electrónicos admitidos.

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

2. El servicio de firma electrónica ejecutará una serie de verificaciones previas a la creación de la firma:

   - ➢ La firma electrónica puede ser validada para el formato del fichero específico que va a ser firmado, según la presente política.

- Los certificados a utilizar han sido expedidos bajo una Declaración de Políticas de Certificación admitida. Se publicarán, en la sede electrónica, la relación de los sistemas de firma y certificados electrónicos admitidos, los procedimientos para los que son válidos y las especificaciones de la firma electrónica que puedan realizarse con los mismos.

- Validez del certificado, comprobando si el certificado ha sido revocado, o suspendido, si entra dentro de su periodo de validez, y la validación de la cadena de certificación, incluyendo la validación de todos los certificados en la cadena.

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

  Si no fuese posible realizar estas comprobaciones, en el momento de la firma, los sistemas correspondientes podrán no aceptar el fichero firmado, o esperar un período de tiempo hasta que se pueda realizar la comprobación.

3. El servicio creará un fichero en formato XAdES para aquellos escenarios en los que sea conveniente. Se recomienda que el fichero resultante tenga una extensión única de forma que los visores de documentos firmados puedan asociarse a esa extensión, haciendo más fácil al usuario el manejo de este tipo de ficheros. Esta extensión podría ser:

   - ✓ .xsig: la firma implementada se ha realizado según el estándar XAdES.

2.4. Verificación de la firma electrónica

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

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

2. Validez de los certificados en el momento en que se produjo la firma, si se trata de una clase de firma que incorpora información sobre revocación de certificados, o en caso contrario, validez de los certificados en el momento de la validación: certificados no revocados, suspendidos, o que hayan expirado, y la validación de la cadena de certificación (incluida la validación de todos los certificados de la cadena). Esta información puede estar contenida en la propia firma en el caso de las firmas longevas.

3. Certificado expedido bajo una Declaración de Prácticas de Certificación admitida en el momento en que se produjo la firma. El listado completo de certificados admitidos puede ser consultado en la sección correspondiente de la sede electrónica.

4. Verificación, si existen, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos.

2.5. Resellado de firmas

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

Esto implica que si queremos tener una firma que pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas existirá un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

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 del estándar correspondiente, 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 se realizará dentro del documento resultante de la firma electrónica. Para ello se utilizará una modalidad de firma 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 deberán aplicar mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente.

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 así como lo especificado en la política de gestión de documentos electrónicos que se aprobará, de acuerdo con lo previsto en el artículo 42 del Decreto de Administración Electrónica.

3. Política de validación de firma electrónica

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

3.1. Identificación del documento

Nombre del documento	Política de firma electrónica basada en certificados de la Administración Pública de la Comunidad Autónoma de Euskadi
Versión	1.1
Identificador de la Política	urn:ejgv:dss:policy:1
URI de referencia de la Política	https://www.euskadi.net
Fecha de expedición	31 de agosto de 2013
Ámbito de aplicación	Ámbito de aplicación del Decreto de Administración Electrónica

3.2. Periodo de validez

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

3.3. Identificación del gestor del documento

Nombre del gestor de la política	Dirección de Atención a la Ciudadanía e Innovación y Mejora de la Administración – Departamento de Administración Pública y Justicia
Dirección de contacto	C/Donostia, 1 01010 Vitoria-Gasteiz

3.4. Control de cambios

Mediante este apartado se pretende ofrecer un seguimiento de todas las versiones por las que ha ido pasando el documento, a fin de tener un control exhaustivo de todos aquellos cambios que se van generando con el paso del tiempo.

Para ello, se muestra una tabla con todas las versiones generadas hasta el momento.

Versión	Fecha	Resumen de los cambios producidos
1	27/07/2012	Primera Versión
1.1	31/08/2013	Añadido nuevo formato de firma: XAdES Enveloping con elemento Manifest

3.5. Usos de firma electrónica

La firma electrónica es un mecanismo para securizar la información a través de los canales telemáticos existentes. El objetivo de la política de firma es indicar los usos que se contemplan para un ámbito y alcance concretos, especificando las condiciones requeridas y necesarias para cada uno de los usos que corresponda.

3.5.1. Firma electrónica de transmisiones de datos

A la hora de transmitir los datos será necesaria la firma electrónica, proporcionando la seguridad en el intercambio y garantizando la autenticación de los actores involucrados en el proceso, así como la integridad del contenido del mensaje de datos enviado y el no repudio de los mensajes entre dos servidores (punto a punto). La firma está asociada al protocolo de transporte, formando parte de los mecanismos de cifrado a implementar en una comunicación segura.

Por lo tanto, toda comunicación que se realice entre las diferentes partes de la administración pública y que requiera el uso de la política de firma definida en este documento deberá firmar los

mensajes SOAP mediante una cabecera Web Service- Security (WSS) para que sean entendidos por la Plataforma Tecnológica para la E-Administración (PLATEA), que se encargará de redirigir estos mensajes SOAP, de forma transparente, a la plataforma de servicios de firma del Gobierno Vasco.

3.5.2. Firma electrónica de contenido

Este tipo de firma equivale, en el entorno digital, a la firma manuscrita tradicional, estando asociada directamente al contenido y garantizando la autenticidad de aquél.

A diferencia de la firma de las transmisiones, la firma de contenido proporciona integridad, autenticación y no repudio entre dos extremos, independientemente de que éste sea intercambiado a través de uno u otro mecanismo.

En caso de intercambio, tanto la firma como el propio contenido irán anexos a la transmisión o intercambio, propiamente dicho. Así, los usos de la firma explicados no son complementarios, sino compatibles, pudiéndose utilizar de forma simultánea.

3.6. 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.

3.6.1. Reglas del firmante

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

3.6.1.1. Formato XAdES

La versión de XAdES contemplada en esta política es la versión 1.3.2, 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.

En el *Anexo II: Estructura de la firma electrónica* se detalla la estructura básica que debe tener una firma electrónica para poder ser considerada válida por el verificador.

Dentro de la política de firma descrita en este documento se admitirán **tres** tipos de firmas, según el ENI:

- ✓ **XAdES Detached:** no incluye el documento original, si no, que se hace referencia a éste a través de una URI que sirve para su localización. Se asociará en las peticiones esta URI con los datos que se envían, es decir, la aplicación cliente es la responsable de proporcionar los datos**.**

  - *NOTA*: La terminología aplicada para este tipo de firma es análoga a la utilizada en otras plataformas como @Firma, denominada: **XAdES Externally Detached**.

- ✓ **XAdES Enveloped:** 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.

- ✓ **XAdES Enveloping con elemento Manifest:** se realizará la firma sobre un hash (indicado como *Manifest*), el cual es un hash de un documento externo a la firma. Este elemento *Manifest* estará ubicado dentro de la firma y lo único que se encontrará fuera de la firma será el documento original sobre el que se realizó el hash.

Los tres tipos de firma podrán tener las siguientes variantes:

- ✓ -T: el documento firmado tendrá, como mínimo, un sello de tiempo que proteja contra el no repudio.

- ✓ -A: modalidad de firma longeva a utilizar para el correcto cumplimiento de la política de firma especificada en el presente documento. Se añade un sello de tiempo periódico tanto a las referencias de certificados y estado de revocación como a los propios certificados y respuestas de revocación.

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>
```

    - 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.

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

- **SignerRole**: define el rol de la persona en la firma electrónica.

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

- **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.

3.6.2. Reglas del verificador

El formato básico de firma electrónica avanzada no incluye ninguna información de validación más allá del certificado firmante, que está incluida en la etiqueta *SigningCertificate*, y de la política de firma que se indique en la etiqueta *SignaturePolicy*.

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, son las siguientes:

- ***SigningTime***: 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.

- ***SigningCertificate***: se utilizará para comprobar y verificar el estado del certificado (y, en su caso, la cadena de certificación) en la fecha de la generación de la firma, en el caso que el certificado no estuviese caducado y se pueda acceder a los datos de verificación (CRL, OCSP, etc.).

- ***SignaturePolicy***: se deberá comprobar, que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que se debe utilizar para un servicio en cuestión.

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

Si se ha realizado una firma que incluye el elemento *Manifest*, el proceso de verificación, además de verificar la firma aportada, deberá comprobar que el hash concuerda con el documento original, de forma que se asegure la integridad del documento original.

El encargado de la verificación de la firma deberá definir sus procesos de validación y de archivado según los requisitos de la política de firma.

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

certificado en el servicio OCSP. Estos tiempos podrán ser variables según el Prestador de Servicios de Certificación.

El sistema correspondiente establecerá el periodo de gracia que está dispuesto a asumir, o si por el contrario el periodo es cero y por tanto no se valida la firma.

3.6.3. Reglas para los sellos de tiempo

El sello 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 **SignatureTimeStamp**.

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

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

3.6.4. Reglas de confianza para firmas longevas

El estándar XAdES (ETSI TS 101 903) contempla la posibilidad de incorporar a las firmas electrónicas información adicional para garantizar la validez de una firma a largo plazo, una vez

vencido el periodo de validez del certificado. Esta información puede ser incluida tanto por el firmante como por el verificador, y se recomienda hacerlo después de trascurrido el periodo de precaución o periodo de gracia. Existen dos tipos de datos a incluir como información adicional de validación:

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

- Certificados que conforman la cadena de confianza.

En el caso de que se deseen generar firmas longevas, se deberá incluir la información de validación, anterior, y añadirle un sello de tiempo. En estos tipos de firma la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

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

3.6.4.1. 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.

El formato **XAdES-X** 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 RevocationValues se recomienda hacer la validación por OCSP ya que estos valores pueden ser muy voluminosos en caso de realizar la validación mediante CRL.

Para el correcto cumplimiento de la política de firma de la Administración Pública de la CAE se deberá usar el formato **XADES-A**, que añade un sello de tiempo a la información anterior, como mecanismo de conservación de firmas longevas.

3.7. Reglas de confianza de certificados de atributos

Esta política de firma no fija ninguna regla específica respecto a los certificados de atributos.

Las políticas de firma particulares de cada organismo o entidad dentro de la CAE, basadas en la presente política marco, podrán fijar reglas específicas para cada uno de los servicios que prestan, siendo necesario cumplir sus requisitos para que la firma sea válida en ese contexto.

3.8. Reglas de uso de algoritmos

Para los entornos de seguridad genérica se tomará la referencia a la URN (Uniform Resource Name) en la que se publican las funciones de hash y los algoritmos de firma utilizados por la especificación XAdES, 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 signatures: Part 1: Hash functions and asymmetric algorithms*".

La presente política admite como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en el estándar XMLDSig.

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).

Para la generación de los sellos de tiempo, se hará uso de sistemas de sellado de tiempo que utilicen una Autoridad de Sellado de Tiempo (*Time Stamping Authority* o TSA). La TSA recibe el documento a sellar, le añade el tiempo actual y lleva a cabo un proceso de firma electrónica mediante un criptosistema asimétrico.

3.9. Reglas específicas de compromisos

Esta política de firma no fija ninguna regla respecto a compromisos específicos.

Las políticas de firma particulares de cada organismo o entidad dentro de la CAE, basadas en la presente política marco, podrán fijar reglas específicas para cada uno de los servicios que prestan, siendo necesario cumplir sus requisitos para que la firma sea válida en ese contexto.

Anexo I: Referencias

Para el desarrollo de su contenido, se ha tenido en cuenta las siguientes especificaciones técnicas:

- ETSI TS 101 903, v.1.3.2. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).
- 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 3275, XML-Signature Syntax and Processing.
- 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".

- CCN-STIC-807: Guía/ Norma de Seguridad de las TIC. Criptología de Empleo en el Esquema Nacional de Seguridad.

Además, se consideran como normativa básica aplicable a la materia:

- 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. 0012-0020).

- 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.

- Ley 56/ 2007 o Ley para el Impulso de la Sociedad de la Información.

- 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 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.

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la ley de propiedad intelectual.

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

- Descripción de los perfiles de certificados de la Ley 11/200, que estarán asociados a esta política de firma: Perfiles de certificados en su última versión disponible.

- Decreto 21/2012, de 21 de febrero, de Administración Electrónica.

- Orden de 27 de Junio de 2012 por la que se aprueba la política de firma electrónica y de certificados.

Anexo II: Estructura de la firma electrónica

Este anexo incluye la estructura básica que se deberá seguir para la generación de una firma electrónica XAdES-EPES, según especificación técnica ETSI TS 101 903, 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 nuevo a través de una adenda a la política.

Formato de firma electrónica avanzada XAdES-EPES

Se utilizan los prefijos *dsig* y *xades* para hacer referencia a los elementos definidos en los estándares XML-Dsig y XAdES, respectivamente.

```
<dsig:Signature ID ? >
                        <dsig:SignedInfo>
                          <dsig:CanonicalizationMethod/>
                          <dsig:SignatureMethod/>
                          (<dsig:Reference URI ? >
                            (<dsig:Transforms/>) ?
                            <dsig:DigestMethod/>
                            <dsig:DigestValue/>
                          </dsig:Reference>) +
                        </dsig:SignedInfo>
                        <dsig:SignatureValue/>
                        (<dsig:KeyInfo>) ?
                        <dsig:Object>
                          <xades:QualifyingProperties>
                            <xades:SignedProperties>
                              <xades:SignedSignatureProperties>
                                xades:SigningTime
                                xades:SigningCertificate
                                xades:SignaturePolicyIdentifier
                                (xades:SignatureProductionPlace) ?
                                (xades:SignerRole) ?
                              </xades:SignedSignatureProperties>
                              <xades:SignedDataObjectProperties>
                                (xades:DataObjectFormat) +
                                (xades:CommitmentTypeIndication) *
                                (xades:AllDataObjectsTimeStamp) *
                                (xades:IndividualDataObjectsTimeStamp) *
                               </xades:SignedDataObjectProperties>
```

```
                    </xades:SignedProperties>
                    <xades:UnsignedProperties>
                        <xades:UnsignedSignatureProperties>
                            (xades:CounterSignature) *
                        </xades:UnsignedSignatureProperties>
                        <xades:UnsignedDataObjectProperties>
                        </xades:UnsignedDataObjectProperties>
                    </xades:UnsignedProperties>
                </xades:QualifyingProperties>
            </dsig:Object>
</dsig:Signature>
```

Los símbolos “+”, “?” y “*” significan:

- ✓ **+** significa una o más ocurrencias
- ✓ **?** significa cero o una ocurrencia
- ✓ ***** significa cero o más ocurrencias

Anexo III: Formato de ficheros admitidos

Este marco de condiciones generales sobre los formatos de fichero de referencia a admitir por las plataformas de relación electrónica de la CAE con la ciudadanía y con otras Administraciones públicas pretende establecer unas consideraciones generales así como la relación de formatos de fichero que deberán ser admitidos por todas las plataformas para facilitar su interoperabilidad. No obstante, 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 establece por el marco normativo de desarrollo del Esquema Nacional de Interoperabilidad tal y como establece la Disposición adicional primera del mismo.

La relación de formatos de documentos electrónicos admitidos se encuentra publicada en la sede electrónica de la Administración Pública de la CAE, en el apartado de documentos electrónicos admitidos.

Consideraciones generales

- ✓ Los formatos de los documentos electrónicos admitidos no deberían obligar a disponer de licencias para visualizarlos o imprimirlos en diferentes sistemas operativos. Se deberían evitar 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.

- ✓ Sería deseable disponer de la posibilidad de comprobar automáticamente el formato y su versión antes de admitirlo en el sistema, es decir, sólo se deberían admitir ficheros cuyo formato pudiera ser comprobado por una máquina antes de su aceptación por el Registro electrónico.

- ✓ Sólo se deberían admitir 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.