# TEXTO CONSOLIDADO DEL DOCUMENTO DE POLITICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS DE LA DIPUTACIÓN PROVINCIAL DE MÁLAGA Y DEL MARCO PREFERENCIAL PARA EL SECTOR PÚBLICO PROVINCIAL

| | |
|---|---|
| Versión | 1.0 |
| Identificador de la política (OID-Objetct IDentifier) | 2.16.724.1.12.1.1.1.1.0 |
| URI (Uniform Resource Identifier) / URL de referencia de la política | https://sede.malaga.es/politica_de_firma_1.0.pdf |
| Fecha de expedición | 19/04/2016 |
| Ámbito de aplicación | Diputación Provincial de Málaga |
| Resoluciones adoptadas | – Acuerdo Plenario de 19/04/2016, punto núm. 1.2.4<br>– Decreto núm. 1406/2016, de 30 de mayo, ordenado por la Presidencia |

INDICE

# 1. CONSIDERACIONES GENERALES

## 1.1. Objeto

La presente política de firma electrónica y certificados tiene por objeto establecer el conjunto de criterios comunes asumidos por la Diputación Provincial de Málaga, en relación con la autenticación y el reconocimiento de firmas electrónicas basadas en certificados. Dicha política constituye a su vez un marco preferencial para todas las entidades dependientes de la Diputación, que integran el Sector Público Provincial.

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

## 1.2. Ámbito de aplicación

Este documento se circunscribe a los certificados previstos en la Ley 11/2007 expedidos para su empleo por la Diputación Provincial de Málaga y los organismos públicos vinculados o dependientes de ésta y a los sistemas de firma electrónica basados en certificados recogidos en el artículo 10.1 y 10.2 del Real Decreto 1671/2009, si bien a partir del 2 de octubre de 2016 entrará en vigor el artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, por lo que serán admitidos los sistemas de firma electrónica que en el mismo identifican.

La política 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 las relaciones con los ciudadanos y entre las Administraciones Públicas.

## 1.3. Normativa y especificaciones técnicas

Como normativa básica aplicable a la materia se ha considerado la siguiente:

- Decisión de la Comisión Europea 130/2011, de 25 de febrero, que establece unos requisitos mínimos para el tratamiento transfronterizo de documentos firmados electrónicamente por las autoridades competentes bajo la Directiva 123/ 2006 relativa a los servicios en el mercado interior.
- 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.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- Política de Firma Electrónica y de Certificados de la Administración General del Estado (URL: https://sede.060.gob.es/politica_de_firma_anexo_1.pdf. Código de verificación electrónico: C4075E8D7946EF14B65819F01C2D5F63).
- Perfiles de certificados electrónicos Documento: Anexo II, Perfiles de certificados electrónicos (URL: https://sede.060.gob.es/perfiles_de_certificados_anexo_2.pdf. Código de verificación electrónico: 483AFA7835C0CF999551DF4992EE945D)
- Resolución de la Secretaría de Estado de Función Pública del 19 de julio de 2011 por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
- 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.
- 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 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.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- 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.
- 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 la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.

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

En la elaboración de la política de firma electrónica se han considerado además las siguientes disposiciones y resoluciones adoptadas por la Diputación Provincial de Málaga:

- Decreto núm. 394/2016, de 2 de marzo, ordenado por la Presidencia, referente a la instrucción para la tramitación electrónica de los permisos de usuarios en la Hacienda Electrónica Provincial (HEP).
- Bases de Ejecución del Presupuesto General 2016 de la Diputación Provincial de Málaga, aprobadas definitivamente el 22 de enero de 2016.
- Acuerdo Plenario de 01/12/2015, punto núm. 1.6.1, referente a la aprobación de la Política de Seguridad de la Información de la Diputación Provincial de Málaga, de conformidad con el Esquema Nacional de Seguridad.
- Decreto núm. 1306/2015, de 8 de mayo, ordenado por la Presidencia, relativo al procedimiento de creación y utilización del sello electrónico de órgano de la HEP.
- Decreto núm. 728/2015, de 12 de marzo, ordenado por la Presidencia, referente a la instrucción para la implantación de la firma electrónica en los procedimientos de la HEP.
- Acuerdo Plenario de 08/05/2012, punto núm. 5.A.4., referente a la aprobación de la Sede y los Registros Electrónicos de la Diputación Provincial de Málaga, de los Ayuntamientos de la provincia, y de sus respectivos entes asociativos o Dependientes, publicado en el BOP de Málaga el 16/07/2012.

Para el desarrollo del contenido de la política de firma electrónica se ha tenido en cuenta las siguientes especificaciones técnicas:

- ETSI TS 101 903, v.1.2.2, v.1.3.2, v.1.4.1. y v.1.4.2. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).
- ETSI TS 101 733, v.1.6.3, v1.7.4 y v.1.8.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 102 778, v 1.2.1. 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. LA POLÍTICA DE FIRMA ELECTRÓNICA

### 2.1. Definición y contenido.

La 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, según define del Real Decreto 4/2010, de 8 de enero. Así pues, en el presente documento se determinan, 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 de la Diputación Provincial de Málaga.

Esta política de firma electrónica resulta de aplicación a toda la Diputación Provincial de Málaga y constituye un marco preferencial para todas las entidades dependientes que integran el Sector Público Provincial, por lo que puede convivir junto con otras políticas

particulares para una transacción determinada en un contexto concreto, siempre basadas en el marco de preferencial o en la política marco de la Administración General del Estado.

### 2.2. Datos identificativos de la política.

El documento de la política de firma de la Diputación Provincial de Málaga queda identificado de la siguiente manera:

a) Nombre del documento: Política de firma electrónica y de certificados de la Diputación Provincial de Málaga.
b) Versión: 1.0
c) Identificador (OID-Objetct IDentifier) de la política: 2.16.724.1.12.1.1.1.1.0, según se establece mediante el Decreto núm. 1406/2016, de 30 de mayo, ordenado por la Presidencia de la Diputación.
d) URI (Uniform Resource Identifier) / URL de referencia de la política: https://sede.malaga.es/politica_de_firma_1.0.pdf
e) Fecha de expedición: La que corresponda a resolución de aprobación.
f) Ámbito de aplicación: Diputación Provincial de Málaga.

El documento de política de firma tiene un identificador único, asignándose los dos últimos dígitos a la versión que corresponda, a fin de distinguir las versiones sucesivas que puedan existir en el caso de que se realicen actualizaciones.

La presente política de firma electrónica será válida desde la fecha de expedición indicada en el apartado anterior, hasta que sea derogada o se publique una nueva versión actualizada, que conllevará también la actualización de la fecha de expedición. Los períodos de transición deberán indicarse en las nuevas versiones actualizadas y transcurridos los plazos indicados únicamente serán válidas las versiones actualizadas. Además, 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.

La Intervención General de la Diputación Provincial de Málaga será el gestor de la presente política de firma electrónica, correspondiéndole el mantenimiento, actualización y, estando ubicado a efectos de notificaciones en la sede de la Diputación Provincial de Málaga en Calle Pacífico 54, 29004 Málaga, y siendo el OID del gestor el que resulte aprobado por resolución de Presidencia.

### 2.3. Actores involucrados en la firma electrónica.

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

a) 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.
b) 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.
c) Prestador de servicios de certificación (PSC): persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
d) 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.

Los propósitos de la firma electrónica basada en certificados son los siguientes:

a) Firma 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.
b) Firma de contenido, como herramienta para garantizar la autenticidad, integridad y no repudio de los mismos, con independencia de que forme parte de una transmisión de datos.

### 2.5. Interacción con otras políticas.

La Diputación Provincial de Málaga ha previsto la adopción de una política de firma propia, en los términos que se expresan en el presente documento de política de firma electrónica y de certificados, estableciéndose la misma como marco preferencial para el Sector Público Provincial.

Los criterios técnicos y organizativos de la política de firma de la Diputación Provincial de Málaga se ajustarán al Esquema Nacional de Interoperabilidad. En el caso de existir

políticas propias en el Sector Público Provincial, las entidades promotoras deberán valorar la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de adoptar la política de firma electrónica y de certificados de la Diputación Provincial de Málaga o la política marco general de la Administración General del Estado, así como determinar la interoperabilidad y las condiciones de utilización y convivencia.

Con la finalidad de asegurar que otras aplicaciones puedan interpretar las reglas que en este documento se determinan, la presente política está disponible en formato XML (eXtensible Markup Language) y ASN.1 (Abstract Syntax Notation One).

### 2.6. Gestión de la política de firma.

La Intervención General actualizará la política de firma atendiendo a las modificaciones motivadas por necesidades propias de la organización, los cambios en políticas relacionadas y/o los cambios en los certificados electrónicos emitidos por los prestadores de servicios de certificación referenciados en la política de firma.

En las revisiones y actualizaciones de las políticas de firma electrónica cooperará e informará el Servicio de Gestión Económica y Presupuestaria, en tanto que en las tareas de mantenimiento y publicación colaborará el Servicio de Nuevas Tecnologías, en cuanto a las responsabilidades que cada uno de ellos asume en la Hacienda Electrónica Provincial y en la Sede Electrónica, o unidades equivalentes en cada caso en el supuesto de existir cambios organizativos.

El Servicio de Nuevas Tecnologías de la Diputación Provincial de Málaga mantendrá en la Sede electrónica (https://sede.malaga.es) la versión actualizada del presente documento y un repositorio con el historial de las versiones anteriores, a fin de proveer la ubicación de las políticas de firma que se hubiesen aprobado.

### 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.

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 deberá existir un servicio que mantenga dichas

evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

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

1. En primer lugar, deberá verificarse la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES y las referencias.
2. Deberá realizarse un proceso de completado de la firma electrónica, consistente en lo siguiente:
    a) Obtener las referencias a los certificados, así como almacenar los certificados del firmante.
    b) Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP, así como almacenarlas.
3. Al menos, deben sellarse las referencias a los certificados y a las informaciones de estado.

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

- en caso de almacenar los certificados y las informaciones de estado dentro de la firma, se recomienda sellar también estas informaciones, siguiendo las modalidades de firmas AdES –X o -A.
- si los certificados y las informaciones de estado se almacenan en un depósito específico, se recomienda sellarlos de forma independiente.

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

- las plataformas de firma electrónica adoptadas en el ámbito de la Diputación Provincial de Málaga 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 permitan 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 (Real Decreto 4/2010, de 8 de enero) y en particular se atenderá a lo establecido en la NTI de Política de gestión de documentos electrónicos.

## 3. REGLAS COMUNES

Las reglas comunes establecen 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.

Estas reglas se definen en base a los formatos de firma electrónica admitidos, teniendo en cuenta los diferentes usos de la firma electrónica basada en certificados, al uso de algoritmos y a los procesos de creación y validación de firma.

### 3.1. Reglas comunes del firmante y del verificador.

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.

#### 3.1.1. Reglas del firmante.

El firmante se hará responsable de que el fichero que se quiere firmar no incorpora 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.

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 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 utilizara 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:

- 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 deben 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 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.

También se permitirá el uso de certificados de atributos para certificar el rol del firmante, en cuyo caso el elemento SignerRole incorporará un elemento CertifiedRoles, que contendrá la codificación en base-64 de uno o varios atributos de certificados del firmante.

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.

### 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 prestador de servicios de certificación (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.

Será responsabilidad del encargado de la verificación de la firma definir sus procesos de validación y de archivado, en consonancia 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.

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

### 3.2. 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.

La Intervención General será la encargada de actualizar las especificaciones relativas a los formatos admitidos en la presente política de firma, prestando su apoyo el Servicio de Gestión Económica y Presupuestaria en las tareas administrativas de los expedientes de revisión, en tanto que en las tareas técnicas de actualización y publicación colaborará el Servicio de Nuevas Tecnologías, o equivalentes en cada caso en el supuesto de existir modificaciones en las unidades organizativas.

El formato de firma electrónica actualmente admitido por la Diputación Provincial de Málaga es XAdES (XML Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 903, en su versión 1.4.2, siendo válidas implementaciones en versiones anteriores que indiquen en tags la versión que se esté utilizando. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

Se tendrá en cuenta la legislación Europea en relación a los formatos de firma admitidos en la Unión Europea, en especial aquellos definidos en los estándares europeos de firma electrónica y por tanto deberá ser actualizada según evolucionen dichas normas Europeas.

La estructura básica que se deberá seguir para la generación de una firma electrónica avanzada básica XAdES EPES es la siguiente:

```
<ds:Signature ID ? >
        <ds:SignedInfo>
                <ds:CanonicalizationMethod/>
                <ds:SignatureMethod/>
```

```
                (<ds:Reference URI ? >
                        (<ds:Transforms/>) ?
                        <ds:DigestMethod/>
                        <ds:DigestValue/>
                </ds:Reference>) +
        </ds:SignedInfo>
        <ds:SignatureValue/>
        (<ds:KeyInfo>) ?
        <ds:Object>
                <QualifyingProperties>
                        <SignedProperties>
                                <SignedSignatureProperties>
                                        SigningTime
                                        SigningCertificate
                                        SignaturePolicyIdentifier
                                        (SignatureProductionPlace) ?
                                        (SignerRole) ?
                                </SignedSignatureProperties>
                                <SignedDataObjectProperties>
                                        DataObjectFormat +
                                        (CommitmentTypeIndication) *
                                        (AllDataObjectsTimeStamp) *
                                        (IndividualDataObjectsTimeStamp) *
                                </SignedDataObjectProperties>
                        </SignedProperties>
                        <UnsignedProperties>
                                <UnsignedSignatureProperties>
                                        (CounterSignature) *
                                </UnsignedSignatureProperties>
                                <UnSignedDataObjectProperties>
                                </UnSignedDataObjectProperties>
                        </UnsignedProperties>
                        </QualifyingProperties>
        </ds:Object>
</ds:Signature>
```

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

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

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 (si el formato del documento original fuese un fichero que contenga sólo texto, fichero XML, no sería precisa su codificación en base64), y las firmas, encontrándose al mismo nivel XML lo firmado y la firma, es decir el modo internally detached.

```
<documento>
        <documentoOriginal Id=”original” encoding=”base64” nombreFichero=nombreFichOriginal”>
```

```
        ...
        </documentoOriginal>
        <ds:Signature>
                <ds:SignedInfo/>
                ...
                <ds:Reference URI="#original">
                </ds:Reference>
                ...
                </ds:SignedInfo>
        ...
        </ds:Signature>
</documento>
```

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

La familia de firmas electrónicas avanzadas XAdES (XML Advanced Electronic Signatures) tienen su origen en el lenguaje de marcas XML (eXtensible Markup Language), desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible, cuyas firmas digitales (XMLDSIG) permiten comprobar que los datos no se modificaron después de firmarlos. A partir del formato básico XAdES existe la posibilidad de generar formas más complejas de firmas electrónicas que incorporan propiedades adicionales y amplían el nivel de protección ofrecido, en el sentido siguiente:

- XAdES-BES (Basic electronic signature). Es una forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada.
- XAdES-EPES (Explicit Policy Electronic Signatures). Esta forma se basa en la anterior (XAdES-BES) a la que se la ha añadido información sobre la política de firma.
- XAdES-T (electronic signature with Time). Es un XAdES-EPES al que se le añade una segunda firma, pero en esta ocasión, una firma realizada por una TSA (Time Stamp Authority). Esta segunda firma aporta información específica sobre la fecha y hora exacta de la firma. El sellado de tiempo se utiliza para proteger contra el repudio.
- XAdES-C (electronic signature with Complete validation data references). Es un XAdES-T al que se le añaden referencias sobre los certificados y listas de revocación (CRL - Certificate Revocation List) utilizadas para la validación del propio certificado utilizado para la firma. Por ejemplo, fue firmado por Certificado XXX emitidos por CA ZZZ y cuya CRL YYYY fue consultada en el momento de la validación.

- XAdES-X (eXtended signatures with time forms). Añade sellos de tiempo a las referencias introducidas por XAdES-C para evitar que pueda verse comprometida en el futuro una cadena de certificados.
- XAdES-X-L (eXtended Long electronic signatures with time). Añade los propios certificados y listas de revocación a los documentos firmados para permitir la verificación en el futuro incluso si las fuentes originales (de consulta de certificados o de las listas de revocación) no estuvieran ya disponibles.
- XAdES-A (Archival electronic signatures). Este formato incluye toda la información anterior pero incluye meta-información asociada a políticas de refirmado. Añade por tanto la posibilidad de timestamping periódico de documentos archivados para prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un periodo largo de almacenamiento.

### 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 la Diputación Provincial de Málaga y otras entidades, que deban cifrarse en una comunicación segura, se hará bajo las especificaciones SOAP, Simple Object Access Protocol, aceptándose al menos 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.

Considerando la Norma Técnica de Interoperabilidad de Catálogo de estándares, el formato para la firma electrónica de contenido en la Diputación Provincial de Málaga será XAdES (XML Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 903, en su versión 1.4.2, y las versiones anteriores.

El perfil mínimo de formato que se utilizará para la generación de firmas de contenido en la Diputación Provincial de Málaga será XAdES-EPES (Explicit Policy Electronic Signatures), por lo que a la forma básica se le añadirá la información sobre la política de firma (XAdES-BES).

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.

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 el caso de la Diputación Provincial de Málaga tomará uno de los siguientes valores:

i. XAdES internally detached signature.

ii. XAdES enveloped signature.

Tal y como se ha señalado en el punto 3.2 (Formatos admitidos de firma electrónica), la firma de facturas electrónicas según el formato «Facturae» se realizará conforme a lo regulado por la Orden PRE/2971/2007, de 5 de octubre.

### 3.5. Reglas de uso de algoritmos.

Para los entornos de seguridad genérica se tomará la referencia a la URN en la que se publican las funciones de hash y los algoritmos de firma utilizados por las especificaciones XAdES, CAdES y PAdES, como formatos de firma adoptados, de acuerdo con las especificaciones técnicas ETSI TS 102 176-1 sobre "Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature". Todo ello sin perjuicio de los criterios que, al respecto, se hayan adoptado en el Esquema Nacional de Seguridad, desarrollado a partir del artículo 42 de la Ley 11/2007, por el Real Decreto 3/2010, de 6 de noviembre.

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.

Asimismo, para garantizar el cumplimiento del Esquema Nacional de Seguridad, se deberá atender a la recomendación CCN-STIC 807 (“Criptografía de Empleo en el ENS”).

Se podrán utilizar cualquiera de los siguientes algoritmos para la firma electrónica: RSA/SHA 1 (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 la Diputación Provincial de Málaga deberán cumplir las siguientes características:

1. El usuario podrá seleccionar un fichero, formulario u otro objeto binario para ser firmado. Los formatos de ficheros atenderán a lo recogido en la NTI de Catálogo de estándares y tendrán en cuenta las siguientes 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.

2. El servicio de firma electrónica ejecutará una serie de verificaciones:
    - Si la firma electrónica puede ser validada para el formato del fichero específico que vaya a ser firmado, según la presente política.

- Si los certificados han sido expedidos bajo una Declaración de Políticas de Certificación específica.
- 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 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", dado que la firma implementada se ha realizado según el estándar XAdES.

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 XAdES, proporcionará la siguiente información (obligatoria):
   a) Fecha y hora de firma. SigningTime (SignedProperties)
   b) Certificado del firmante. SigningCertificate (SignedProperties)
   c) Política de firma sobre la que se basa el proceso de generación de firma electrónica. SignaturePolicyIdentifier-SigPolicyId (SignedProperties) / SignaturePolicyIdentifier-SigPolicyHash (SignedProperties)
   d) Formato del objeto original. DataObjectFormat (SignedProperties)

5. Como datos opcionales, la firma electrónica podrá incluir:
   a) Lugar geográfico donde se ha realizado la firma del documento. SignatureProductionPlace (SignedProperties)
   b) Rol de la persona firmante en la firma electrónica. SignerRole-ClaimedRoles (SignedProperties)

c) Acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.). CommitmentTypeIndication (SignedProperties)
d) Sello de tiempo sobre algunos o todos los objetos de la firma. AllDataObjectsTimeStamp (SignedProperties) / IndividualDataObjectsTimeStamp (SignedProperties)

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.

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

1. Garantía de que la firma es válida para el fichero específico que está firmado.
2. Validez de los certificados en el momento en que se produjo la firma, si los servicios de los prestadores facilitan los históricos de estado de los certificados, o en caso contrario, validez de los certificados en el momento de la validación: certificados no revocados, suspendidos, o que hayan expirado, y la validación de la cadena de certificación (incluida la validación de todos los certificados de la cadena). Esta información puede estar contenida en la propia firma en el caso de las firmas longevas.
3. Certificado expedido bajo una Declaración de Prácticas de Certificación específica.
4. Verificación, si existen y si así lo requiere la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos.

Para validar la firma electrónica se considerará la siguiente información:

a) Fecha y hora de la firma: 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. En caso de que no existan sellos de tiempo, la fecha y hora de la firma tendrán carácter indicativo, pero no se utilizarán para determinar el momento en que se

realizó la firma. En caso de que no existan sellos de tiempo en la firma, la validación del certificado se realizará en el momento de la validación de la firma.

b) Certificado del firmante. Este campo se utilizará para verificar el estado del certificado, y en su caso la cadena de certificación, en la fecha de la generación de la firma.
c) Política de firma sobre la que se basa el proceso de generación de firma electrónica. Se utilizará para identificar, mediante su hash y su identificador (OID), que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que se utilizará para el servicio en cuestión.

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

Para la verificación del estado de los certificados en el caso de formatos de firma longeva, la validez de la firma vendrá determinada por la validez del sello de tiempo de las evidencias de la validación incluidas en la firma.

## 4. REGLAS DE CONFIANZA

### 4.1. Reglas de confianza de certificados electrónicos.

Se consideran válidos para ejecutar la firma electrónica de contenido los certificados reconocidos según la Ley 59/2003, de 19 de diciembre, y la Directiva 1999/93/CE de 13 de diciembre de 1999, las nuevas tipologías de certificados definidos en la Ley 11/2007, de 22 de junio, así como los sistemas de firma y certificados electrónicos indicados en el artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, por lo que serán admitidos los siguientes:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.
b) Sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Otro sistemas que la Diputación Provincial de Málaga pueda considerar válido para realizar determinados trámites o procedimientos de su ámbito de competencia, en los términos y condiciones que se establezcan.

Los certificados de firma electrónica de empleado público emitidos por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) se consideran válidos para la realización de firma electrónica por parte del personal de la Diputación Provincial de Málaga, por lo que resultan ser adecuados para garantizar la identificación y firma de los participantes en la tramitación de cuantos procedimientos electrónicos se determinen.

Desde la aprobación del Decreto núm. 728/2015, de 12 de marzo, ordenado por la Presidencia, la Diputación se encuentra en inmersa en un proceso de implantación y uso de la firma electrónica para miembros y empleados públicos de la Diputación de Málaga, implicados en los procedimientos de la Hacienda Electrónica Provincial. Por razones de seguridad pública, los sistemas de firma electrónica harán referencia al número de identificación profesional del empleado público y al órgano en donde presta sus servicios, en virtud de las potestades reconocidas en el Art. 43.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Junto a los certificados del personal, la Diputación también se ha dotado de instrumentos para la actuación administrativa automatizada, habiéndose iniciado en esta labor mediante el Decreto núm. 1306/2015, de 8 de mayo, por el que se establece el procedimiento de creación y utilización del sello electrónico de órgano de la Hacienda Electrónica Provincial. De acuerdo con lo dispuesto en el Art. 40.1 de la  de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, los certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos. Además, tal y como dispone el Art. 41.2 de la anterior norma, en caso de actuación administrativa automatizada se deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

La relación de sellos electrónicos utilizados por la Diputación Provincial de Málaga, incluyendo las características de los certificados electrónicos y los prestadores que los expiden será pública y accesible a través de la sede electrónica. Además, la verificación de sus sellos y certificados electrónicos, incluyendo el de la propia sede, se podrá efectuar a través de la aplicación de Validación de firma y certificados Online y Demostrador de servicios de @firma (https://valide.redsara.es) u otros sistemas reconocidos de validación electrónica.

### 4.2. Reglas de confianza para los sellos 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 puede ser añadido por el emisor, el receptor o un tercero y se debe incluir como propiedad no firmada en el campo Signature Time Stamp.

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

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

### 4.3. Reglas de confianza para firmas longevas.

Los estándares 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 periodo de validez del certificado. Esta información puede ser incluida tanto por el firmante como por el verificador, y se recomienda hacerlo después de transcurrido 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 deberá usar validación mediante OCSP (Online Certificate Status 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 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.

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 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.