POLÍTICA DE FIRMA ELECTRÓNICA

DE LA DIPUTACIÓN PROVINCIAL

DE CASTELLÓN

TEXTO CONSOLIDADO
Última modificación: 31 de marzo de 2015.

ÍNDICE

1. INTRODUCCIÓN.

La Diputación de Castellón en su estrategia de implantación de la Administración electrónica y, en relación con los documentos y expedientes electrónicos, requiere dotarse de una Política de Firma Electrónica y del uso de certificados digitales tal y como establece la resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración pública.

Esta Política de Firma Electrónica debe garantizar el correcto uso de herramientas de firma electrónica con el objetivo de que permitan generar con carácter de autenticidad documentos electrónicos, expedientes electrónicos y foliados de expedientes electrónicos. Para ello esta política se fundamenta en los siguientes criterios:

- La vocación de la Diputación en que su actividad administrativa pueda plasmarse en documentos y expedientes electrónicos auténticos, por lo que en un futuro se pueda implantar la Administración sin papeles.
- Los documentos firmados electrónicamente, en cumplimiento de lo establecido en esta política, tendrán plena validez y se considerarán originales y definitivos.
- El nivel de seguridad tecnológica, el tipo de certificado a utilizar, el formato de la firma y los mecanismos de preservación se fijarán en función de la importancia del documento y del acto administrativo a que se refieran.
- En la medida de lo posible, las firmas electrónicas que se generan en la Diputación se harán, en origen, con el formato y nivel de seguridad requerido para su conservación durante todo el periodo de vida útil del documento al que hacen referencia. Del mismo modo, los documentos electrónicos que se reciban firmados serán sometidos a un proceso de validación y compleción de las firmas en el momento de la recepción.

En este sentido, en esta Política de Firma Electrónica se desarrollan los siguientes elementos:

1. El objeto con el que se desarrolla la Política de firma electrónica.

2. Los datos identificativos de la política, sus periodos de validez y su transición a nuevas políticas y la asignación de responsabilidades para su gestión.
3. La definición de los conceptos clave en materia de firma electrónica y que son desarrollados a lo largo de la Política.
4. La normativa y estándares internacionales a la que está sujeta la Política de firma electrónica de la Diputación y en base a la cual se desarrolla.
5. El uso de certificados digitales:
    - Certificados digitales admitidos: qué certificados digitales pueden utilizar otras personas o entidades para relacionarse telemáticamente con la Diputación, y como se actualizará y publicará la lista de certificados admitidos.
    - Certificados digitales empleados: qué certificados digitales pueden utilizar los empleados de la diputación, en el ejercicio de sus funciones, y los sellos electrónicos están previstos para la actuación automatizada.
6. El ciclo de vida de los certificados empleados por la Diputación, identificándose cómo pueden obtenerse estos cuando se necesiten y cómo se llevará el control de los certificados existentes y de su eventual revocación cuando dejen de ser necesarios.
7. La definición del sello de tiempo como elemento que permite dejar evidencia de la fecha y hora en que se ha producido un acto.
8. Las clases, tipos y niveles de firma, es decir, el cómo y en qué formato se generan las firmas electrónicas empleadas en el ámbito de la Diputación y el proceso seguido para su validación.
9. El mantenimiento y la preservación de firmas electrónicas para garantizar la introducción en los sistemas de gestión documental de la Diputación de documentos auténticos que garanticen la preservación de su validez jurídica a largo plazo mediante procesos de resellado de tiempo.
10. La identificación de los metadatos previstos en el Vocabulario de Metadatos de la Diputación de Castellón para la gestión efectiva de firmas electrónicas.

11. Las normativas de firma electrónica aplicados en un contexto particular que tienen por objetivo determinar la validez de una firma electrónica en una transacción particular identificándose qué obligaciones asume la Diputación en cada caso, teniendo en cuenta el uso que debe darse a los objetos firmados electrónicamente, documentos o expedientes electrónicos, y el tipo de actuación administrativa que recoge el acto de firma.
12. La identificación de un subconjunto representativo de casos de uso de la firma electrónica que identifican posibles escenarios en los que los procedimientos de la Diputación pueden requerir el uso de firmas electrónicas vinculado a una normativa de firma electrónica concreta:
    - Foliado de expedientes electrónicos.
    - Firma electrónica de un documento electrónico.
    - Digitalización certificada de documentos en papel.
    - Copia auténtica electrónica de un documento firmado electrónicamente.
    - Procesos de firma automatizada.
    - Tratamiento de documentos firmados electrónicamente y aportados por terceras partes.

Para la elaboración de esta Política de Firma Electrónica se ha tenido en cuenta lo que el Esquema Nacional de Interoperabilidad establece al respecto y, muy concretamente, lo que se define en la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados digitales de la Administración, así como la del expediente electrónico en lo referente a la firma electrónica de los mismos.

2. OBJETO DE LA POLÍTICA DE FIRMA ELECTRÓNICA.

La Política de Firma Electrónica tiene por objeto establecer el conjunto de criterios comunes asumidos por la Diputación de Castellón en relación con la autenticación y el reconocimiento de firmas electrónicas basadas en certificados digitales. En concreto establece las directrices a seguir por la Diputación de Castellón respecto al uso de la firma electrónica, en el seno de las aplicaciones informáticas corporativas, para garantizar la autenticidad, integridad y conservación de los documentos electrónicos firmados digitalmente.

Asimismo, el objetivo de esta política es establecer qué certificados digitales de ciudadano la Diputación acepta y qué certificados digitales utilizan los trabajadores de ésta y, además, sobre estos últimos certificados, su ciclo de vida.

Por último, establece las estrategias que la Diputación utilizará para la preservación a largo plazo de las firmas electrónicas.

3. DATOS DE LA POLÍTICA DE FIRMA ELECTRÓNICA.

3.1 Identificación de la política.

Los datos identificativos de la Política de Firma Electrónica son los que se incluyen a continuación:

1. Nombre del documento: Política de Firma Electrónica de la Diputación de Castellón.
2. Versión: 1.0
3. Fecha de aprobación: 31 de marzo de 2015

3.1.1 Periodos de validez y transición.

La presente Política de Firma Electrónica de la Diputación de Castellón entrará en vigor en la fecha de su aprobación y será válida hasta que no sea sustituida o derogada por otra política posterior.

Si se estima oportuno, una nueva versión de la Política de gestión documental podrá facilitar un período de tiempo transitorio para adecuar los diferentes sistemas de firma electrónica y validación utilizados por la Diputación de Castellón a las especificaciones de la nueva versión.

Este período de tiempo de transición se deberá indicar en la nueva versión y superado el mismo sólo será válida la versión actualizada.

3.1.2 Identificación del gestor del documento de la política.

A continuación se incluyen los datos identificativos del gestor de la Política de Firma Electrónica de la Diputación de Castellón:

1. Responsable de la política: Secretaría General
2. Dirección de contacto: Plaza las Aulas, 7, Castellón
3. e-mail de contacto: actas@dipcas.es

4. Teléfono de contacto: 934 359 909

4. CONCEPTOS.

Se incluye a continuación la definición de términos, aplicados en este documento, para hacer más comprensible el documento de Política de Firma Electrónica de la Diputación de Castellón.

Autoridad de certificación: Es una persona física o jurídica que, cumpliendo con los requisitos que determina la legislación establecida sobre firma electrónica, está capacitada para la emisión y la gestión (renovación, suspensión y revocación) de certificados electrónicos con las máximas condiciones de seguridad y de calidad. Son funciones básicas de las autoridades de certificación:

- Verificar la identidad de los solicitantes de certificados.
- Publicar las listas de revocación de certificados. Las especificaciones se describen en la norma ISO/IEC 9594-8.

La legislación española establece que las Autoridades de certificación cumplen con la función de "tercera parte de confianza" ya que garantizan a los usuarios de su infraestructura que los sujetos que se relacionan a través de medios telemáticos son quién dicen ser sin posibilidad de error.

Casos de uso de la firma electrónica: En este documento nos referimos a los casos de uso de la firma electrónica, a los escenarios posibles de generación de documentos electrónicos firmados. Para cada caso de uso se identificarán los formatos de firma electrónica, los posibles niveles de firma, la normativa de firma electrónica a aplicar, etc.

Certificado digital: Según la Ley 59/2003, de firma electrónica, un certificado digital es un documento electrónico firmado digitalmente por un prestador de servicios de certificación que vincula unos datos de verificación de firma (clave pública) con un firmante, confirmando así su identidad en el mundo electrónico. Por lo tanto, permite identificar electrónicamente una persona en Internet y a ésta emitir firmas electrónicas con plena validez jurídica.

Clases de firma electrónica: En este documento nos referiremos a las clases, a la validez jurídica de la firma electrónica, según se define en la Ley 59/2003 de firma electrónica: firma simple, avanzada y reconocida.

Documento electrónico: Es el documento redactado en soporte electrónico y que contiene datos firmados electrónicamente. Los documentos electrónicos serán el soporte de documentos públicos, de documentos expedidos y de documentos privados.

Firma electrónica: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, "conjunto de datos en forma electrónica, consignados juntamente con otros o asociados con otros, que pueden ser utilizados como medio de identificación del firmante".

Existen los siguientes tipos de firma electrónica:

- Firma electrónica avanzada: firma electrónica que permite identificar el firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha estado creada por medios que el firmante puede mantener bajo su control exclusivo.
- Firma electrónica reconocida: firma electrónica basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Esta firma tendrá respecto a los datos consignados electrónicamente el mismo valor que la firma manuscrita respecto a los datos consignados en papel.

Formato de firma electrónica: Forma en que se codifican las firmas electrónicas. Los formatos más utilizados son los formatos S/MIME, CMS, XAdES, CAdES y PAdES.

Nivel de firma: Con este nombre nos referiremos a si el documento tiene una única firma o múltiples firmas y en este caso si se generan en paralelo o anidadas.

Normativa de firma electrónica: Documentos que detallan las 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 los diferentes tipos de transacción.

Resumen criptográfico: Es la función por la cual se garantiza la integridad de un documento electrónico, es decir, que un documento electrónico no ha sido

modificado o manipulado, sin que quede constancia. La normativa ISO-10118-3:2004 establece las especificaciones de las funciones de hash o resumen criptográfico las cuales cumplen con estas tres características:

- Partiendo del resumen/hash es imposible recuperar el documento original.
- Cualquier cambio en el documento original nos dará un resumen/hash diferente.
- Dos documentos originales diferentes tendrán resúmenes/hashs diferentes.

Revocación de certificados digitales: La revocación de un certificado implica la extinción de su vigencia y la pérdida de su validez. La revocación puede ser solicitada por el firmante, la persona física o jurídica representada por éste o por una Entidad de registro en casos como la pérdida del soporte físico del certificado o cualquier indicio de uso fraudulento.

Sello de tiempo: El sello de tiempo asocia un documento, mediante una fuente fiable, con la fecha y la hora en que se generó. Por lo tanto, acredita, a nivel técnico y jurídico, el contenido de un documento electrónico en un cierto momento del tiempo. La acreditación efectuada mediante un sello de tiempo siempre es realizada por un tercero de confianza.

Tipos de firma: Forma como se relaciona la firma electrónica con el documento firmado: dentro del mismo documento, como un documento a parte o dentro de estructuras XML.

5. NORMATIVA APLICABLE Y ESTÁNDARES INTERNACIONALES.

La reciente revolución en el uso del documento electrónico es el resultado de la aparición de cambios normativos que han dado impulso a las herramientas telemáticas y han equiparado, en determinadas circunstancias, los documentos en formato electrónico a los documentos en formatos más tradicionales.

Además, tanto a nivel nacional como en la Unión Europea o internacionalmente, las organizaciones de estandarización técnica han definido y documentado los criterios y formatos que se utilizarán para la gestión de los documentos digitales en todos sus aspectos, garantizando su validez jurídica.

En este apartado se identifican el conjunto de normativas y estándares internacionales que se han tenido en cuenta para la definición de la Política de Firma Electrónica de la Diputación de Castellón.

Para mayor detalle de estas normativas y estándares nos referimos al Modelo de Gestión de Documentos Electrónicos de la Diputación de Castellón donde se incluye el marco normativo completo que afecta a la gestión de documentos electrónicos.

5.1 Normativa aplicable.

- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- Real Decreto 1720/2007, de Desarrollo Parcial de la Ley 11/2007
- Real Decreto 3/2010, de 8 de enero, del Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, del Esquema Nacional de Interoperabilidad.
- Resolución de 19 de julio de 2011, de la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
- Resolución de 19 de julio de 2011, de la Norma Técnica de Interoperabilidad de Expediente Electrónico.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Real Decreto 14/1999, de 17 de septiembre, por el que se que Regula el uso de la firma electrónica.
- Ley 15/2015, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa.
- Directiva 1999/93/CE, de 13 de diciembre, del Marco comunitario para la firma electrónica.
- Regulación (EU) 910/2014, de 23 de julio de 2014, sobre identidad electrónica y servicios de confianza para las transacciones electrónicas en el mercado interno relativas a la Directiva 1999/93/CE.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

5.2 Estándares internacionales y otras convenciones.

- ETSI RFC 2315 (1998), ETSI RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS#7: Cryptographic Message Syntax (CMS)
- ETSI TS 101 733. v.1.6.3, v1.7.4 y v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
- IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP
- ETSI TS 101 903 v.1.2.2, v.1.3.2 y 1.4.1: XML Advanced Electronic Signatures (XAdES)
- IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures.
- ISO 19005 (2008): Formato de fichero PDF/A-1
- ISO/TR 18492: 2005- Long-term preservation of electronic document-based Information
- UNE-ISO/TR 13008: 2010- Información y documentación. Conversión de documentos digitales y procesos de migración.
- 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 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".

6. USO DE CERTIFICADOS DIGITALES.

6.1 Certificados admitidos por la Diputación.

El mecanismo de firma electrónica se sustenta en la existencia de Autoridades de Certificación que emiten certificados digitales y permiten comprobar que un certificado concreto ha estado correctamente emitido y que continúa siendo válido en el momento de su uso, es decir, de la firma de un documento o de la identificación fehaciente de una persona, entidad o proceso en un entorno digital.

La relación entre la Autoridad de Certificación y la entidad que valida el certificado es una relación que se fundamenta en la confianza: los certificados serán aceptados sólo en la medida en que la entidad que lo ha de validar confíe en la honestidad de la Autoridad de Certificación.

En este contexto, la Diputación debe, según la Ley 15/2015, admitir todos los certificados digitales emitidos por los prestadores de servicios de certificación que

hayan realizado la comunicación prevista en el artículo 30.2 de la Ley 59/2003 en el Ministerio de Industria, Energía y Turismo y que cumplan con los estándares de calidad y niveles de seguridad establecidos por dicho Ministerio.

No obstante, en este ámbito la Diputación está utilizando la plataforma @firma del Ministerio de Industria, Energía y Turismo para la validación de los certificados, por lo que la aceptación efectiva de certificados vendrá condicionada por la actualización de los servicios de dicha plataforma.

Debido a ello, aunque la Ley 15/2015 exime de esta responsabilidad, en la Sede Electrónica de la Diputación se publicará la lista de certificados admitidos que se irá actualizando hasta que puedan ser admitidos todos los certificados digitales reconocidos por el Ministerio de Industria, Energía y Turismo, momento en que se procederá a su despublicación. Para su facilidad de gestión y mantenimiento actualizado, este listado se vinculará con el listado publicado por el Centro de Transferencia de Tecnología en el documento “Anexo – Proveedores de servicios de Certificación” accesible a través del Portal de Administración electrónica en el siguiente enlace:

http://administracionelectronica.gob.es/ctt/afirma/descargas#.VGU_EvmG-So

Finalmente, con el objetivo de promover el uso del certificado digital, la Diputación de Castellón se ha constituido en distintas dependencias físicas como Punto de Registro de Usuarios de la ACCV con el objetivo de facilitar la obtención de certificados digitales, en soporte software, tanto a ciudadanos como a empresas como a empleados públicos de los Ayuntamientos de la provincia de Castellón. De las dependencias físicas en las que es posible realizar la solicitud de un certificado y el horario en que puede realizarse se informará debidamente en la Sede electrónica de la Diputación.

Con el objetivo de formalizar la relación entre la Diputación y la ACCV se ha suscrito el correspondiente convenio entre ambas partes.

6.2 Certificados empleados por la Diputación.

Los empleados de la Diputación que deban firmar documentos digitalmente o tener acceso a determinados servicios o aplicaciones donde se requiera un alto nivel de autenticación, necesitarán certificados digitales. Para este propósito la Diputación de Castellón utilizará certificados de empleado público de la Agencia de Certificación de la Comunidad Valenciana (ACCV) basados en tarjeta criptográfica.

No obstante, debido a las falta de interoperabilidad de ciertas aplicaciones de las AAPP, la Diputación también podrá utilizar certificados digitales emitidos por la FNMT y por Seguridad Social, para la relación de la Diputación con otras Administraciones públicas.

En lo referente a los sellos electrónicos, de órgano y de Sede electrónica, la Diputación utilizará los de la Agencia de Certificación de la Comunidad Valenciana y se generarán desde la entidad de registro de la Diputación.

Todos estos certificados digitales son solicitados de forma centralizada desde el Servicio de Administración e Innovación Pública de la Diputación de Castellón a la ACCV u Autoridad de Certificación correspondiente y emitidos directamente por esta última sin que participen los Puntos de Registro de Usuarios de la ACCV que la Diputación tiene constituidos. Para mayor detalle nos referimos al siguiente apartado de esta Política referente al ciclo de vida de los certificados digitales empleados por la Diputación.

En lo que respecta al uso de certificados digitales de servidor, los utilizados para el intercambio seguro de información entre Administraciones públicas se utilizará también los de la Agencia de Certificación de la Comunidad Valenciana, o en su defecto, cualquiera de los emitidos por otras autoridades de certificación que ya tengan un alto nivel de instalación, de sus claves públicas, en los navegadores. Cabe señalar que si bien estos certificados no generan actos jurídicos, se ha considerado oportuno incorporarlos a esta política.

Finalmente, los certificados utilizados por la Diputación han sido comunicados al Ministerio de Industria, Energía y Turismo, por parte de la ACCV o Autoridad de Certificación correspondiente, de acuerdo a lo que prevé el artículo 30.2 de la Ley 59/2003, de Firma Electrónica.

7. CICLO DE VIDA DE LOS CERTIFICADOS DIGITALES EMPLEADOS POR LA DIPUTACIÓN.

Como ya se ha señalado, la Diputación ha determinado que sea el Servicio de Administración e Innovación Pública el punto centralizado para la solicitud de emisión de los certificados digitales que requiera en la realización de sus actividades. Estos certificados digitales son emitidos mayoritariamente por la ACCV, pero también pueden ser emitidos por otras Autoridades de Certificación.

La ACCV o, en su defecto, la Autoridad de Certificación que haya emitido un certificado digital para uso en el seno de las actividades de la Diputación, es la responsable de definir las políticas de gestión de los certificados digitales que emite y por tanto es quien define la vigencia de los certificados, la manera como se revocan, se renuevan, se validan, etc. En definitiva, todo lo que tiene que ver con la gestión del ciclo de vida de los certificados digitales.

Para la emisión de certificados digitales, la Diputación dispone de una tipología de expediente específica implementada sobre el gestor de expedientes electrónicos GESTIONA. El flujo de tramitación que permite esta tipología de expediente consiste en:

1. Para la emisión de un nuevo certificado digital de trabajador público:
    - El usuario que requiera de un certificado deberá iniciar el trámite de solicitud. En la petición se deberá consignar todos los datos necesarios para la emisión del certificado digital; NIF y nombre completo de la persona para la que se emite.
    - El responsable inmediato de este usuario autorizará la solicitud mediante documento de autorización firmado electrónicamente.
    - En última instancia, la solicitud será aprobada por la Secretaría de la Diputación quedando constancia mediante documento de resolución firmado electrónicamente por la Secretaría.
    - El Servicio de Administración e Innovación Pública cursará la petición a la ACCV haciendo uso de un formulario electrónico provisto por la misma ACCV e intercambiado vía correo electrónico.
    - La ACCV iniciará el proceso de emisión y entrega del certificado digital.
    - El empleado recibirá el certificado digital directamente desde la ACCV y deberá firmar manuscritamente el documento correspondiente al contrato con la ACCV y que además deberá digitalizar de forma segura para anexar al expediente electrónico dentro de GESTIONA.
2. Para la emisión de un nuevo certificado digital de persona jurídica, de sello de órgano o de representación de la Diputación:

- El Servicio de Administración e Innovación Pública identificará la necesidad y dará inicio a un expediente de solicitud de certificado digital a través de GESTIONA.
- Si la necesidad es identificada por un departamento diferente al de Administración e Innovación Pública se cursará como en el caso anterior la correspondiente petición a través de GESTIONA por parte del responsable del departamento y, previa a la autorización de Secretaría, existirá una validación por parte del departamento de Administración e Innovación Pública.
- En el caso de los certificados de sello de órgano o de persona jurídica será necesario identificar los datos de la persona responsable del certificado digital; NIF y nombre completo.
- En el caso del certificado de representación de la Diputación será necesario identificar los datos de la persona para la que se emite el certificado digital, NIF y nombre completo, así como el cargo que ocupa en la Diputación y el documento acreditativo relacionado.
- En última instancia cualquier solicitud será aprobada por la Secretaría de la Diputación mediante documento de resolución firmado electrónicamente.
- Finalmente, el Servicio de Administración e Innovación Pública cursará la petición a la ACCV haciendo uso de un formulario electrónico provisto por la misma ACCV e intercambiado vía correo electrónico.
- La ACCV iniciará el proceso de emisión y entrega del certificado digital.
- La recepción de certificados digital de esta tipología y su posterior distribución interna se centralizará en el Servicio de Administración e Innovación Pública.

3. Para la emisión de un nuevo certificado digital de Sede electrónica o de servidor seguro:
   - Se procederá de igual forma que en el caso anterior con la particularidad de que será necesario identificar la URL u otra

información de carácter técnico que permitirá identificar el certificado digital que sea requerido.

En relación a certificados digitales emitidos por otras Autoridades de Certificación diferentes a la ACCV, necesarios para responder a necesidades puntuales de la Diputación, se aplicará el mismo procedimiento implementado sobre GESTIONA, pero siendo necesario justificar mediante documento firmado electrónicamente por el responsable de la petición el motivo por el que no se puede emplear un certificado digital emitido por la ACCV. El Servicio de Administración e Innovación Pública deberá validar la solicitud que será autorizada en última instancia por la Secretaría de la Diputación. Finalmente, el Servicio de Administración e Innovación Pública cursará la solicitud mediante el servicio que establezca la Autoridad de Certificación emisora del certificado digital.

Para la gestión de los certificados digitales durante su vida útil, el Servicio de Administración e Innovación Pública de la Diputación dispondrá de un inventario actualizado el cual, entre otros datos, incluye el número de certificado, el tipo de certificado, el emisor del certificado, la persona o aplicación que gestiona el certificado así como la fecha de caducidad del certificado. Con el soporte de este inventario se realizarán controles proactivos para:

- Renovar aquellos certificados digitales cuya finalidad siga existiendo en el momento próximo a su caducidad y antes de que caduquen o comunicarlo a la persona responsable de iniciar el proceso de renovación.
- En conjunción del departamento de Recursos Humanos revocar aquellos certificados digitales de personal que deje de formar parte de la Diputación o cambie de puesto de trabajo y no requiera del certificado digital.
- En cambios del equipo de gobierno se hace una revisión de todos los certificados digitales de los cargos y se revocan los certificados innecesarios y se emiten los adicionales que resulten necesarios.
- Periódicamente se revisan los certificados disponibles distintos a los de empleado público y, en caso de no ser necesarios, se procede a su revocación.

Adicionalmente, el usuario será informado convenientemente de su responsabilidad en relación a la custodia segura del certificado digital y de los procedimientos que debe seguir en casos en que la integridad del certificado digital pueda ser puesta en duda, como por ejemplo si lo extravía. Para hacerlo

posible al usuario, conjuntamente con el certificado digital, se le entregará y firmará copia de las políticas de uso del certificado digital emitidas por la Autoridad de Certificación emisora del certificado digital. Esta documentación será custodiada digitalizada de forma segura en el expediente de GESTIONA correspondiente a la solicitud del certificado.

8. SELLO DE TIEMPO.

El sello de tiempo es una firma electrónica generada por un tercero de confianza de acuerdo con un certificado digital especialmente destinado al efecto.

Las características principales del sello de tiempo deben consistir en:

- Evidencia de la fecha y hora en que se ha producido un acto. Se utiliza conjuntamente con un documento en cualquier formato y que puede estar firmado electrónicamente. El sello de tiempo puede hacer referencia a la:
    - Firma del documento: el sello de tiempo está asociado a la firma electrónica.
    - Creación del documento: el sello de tiempo está asociado al documento.
- Mediante un proveedor de sellado de tiempo, se sellará la fecha y hora del instante en el que se ha realizado el acto. El proveedor de sellado de tiempo de la Diputación de Castellón será la Autoridad de Certificación de la Comunidad Valenciana.
- Se deberá disponer de un proveedor de sello de tiempo alternativo para garantizar la disponibilidad de los procedimientos de sellado de tiempo. Estos proveedores deben estar sincronizados con la fuente fiable de tiempo de la Real Armada Española según reconoce el Esquema Nacional de Interoperabilidad. Existen diversas fuentes de sellado de tiempo en el mercado, y habrá que escoger las que más convengan dependiendo de: disponibilidad del servicio, calidad del proveedor, coste del servicio, posibilidad de firma de acuerdos de nivel de servicio y autoridad certificada para este servicio.
- El proceso de sellado de tiempo consiste en crear una evidencia electrónica sobre una firma electrónica: se calcula el resumen criptográfico o “hash” del documento y/o sus firmas electrónicas (en el caso del

resellado). Es decir, se trata de una operación matemática que se aplica al conjunto de información sobre el que emitir el sello de tiempo y obtiene una cadena de bits, el "hash", la cual se cifra con la clave privada del certificado de sello de tiempo utilizado para hacer la operación. Esta firma electrónica es devuelta conjuntamente con la fecha y hora de la operación, así como con la información sobre el certificado de sello de tiempo utilizado para hacer la firma el cual incluye la clave pública del certificado que permitirá vincular el sello de tiempo con el tercero de confianza que lo ha emitido.

9. CLASES, TIPOS Y NIVELES DE FIRMA.

En este apartado se recopilan los aspectos relacionados con la firma electrónica en el marco de la Diputación de Castellón, incluyendo los diferentes usos de la firma electrónica en el ámbito de sus sistemas.

Antes de ello, resulta necesario reconocer que los objetivos que persigue la Diputación con la implantación de la firma electrónica son fundamentalmente tres:

- Dotar a la Diputación de un sistema para el control, el uso y la conservación de la documentación origina firmada electrónicamente, gestionada en el desarrollo habitual de su actividad política y administrativa.
- Garantizar la gestión adecuada de los documentos de la Diputación, asegurando la autenticidad, la fiabilidad, la integridad y la disponibilidad futura a lo largo de su ciclo de vida, basado en un software informático que ofrece una capa de gestión de documentos y archivo común.
- Dar respuesta a las exigencias en materia de archivo electrónico de la Ley 11/2007, de 22 de junio, y del Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.

Una vez sentados estos objetivos básicos, hay que tener presente la definición de las **clases o tipos de firma** desde un punto de vista jurídico y técnico.

Desde un punto de vista jurídico existen las siguientes clases de firma:

- **Firma electrónica ordinaria o básica**: es el conjunto de datos en forma electrónica, consignados conjuntamente con otros o que están asociados, que pueden ser utilizados como medio de identificación del firmante (donde identificación debe entenderse como autenticación de entidades, según lo

que establece la Directiva 99/93/CE, de 13 de diciembre, de firma electrónica).

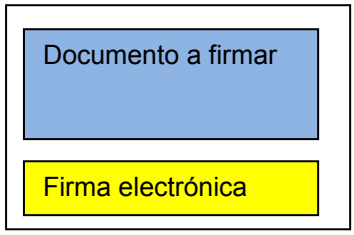
- **Firma electrónica avanzada**: es la firma electrónica que permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a los que hace referencia y que ha estado creada por medios que el firmante puede mantener bajo su control exclusivo.
- **Firma electrónica reconocida**: es la firma electrónica avanzada que se basa en un certificado reconocido y que ha estado generada mediante un dispositivo seguro de creación de firma, según establece el artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Para las definiciones anteriores, se utiliza el concepto clave de certificado reconocido que según la Ley 59/2003, de firma electrónica, en su artículo 11.1, se define como aquellos certificados electrónicos emitidos por un prestador de servicios de certificación, que cumplen con los requisitos establecidos en la misma Ley en cuanto a la comprobación de la identidad y el resto de circunstancias de los solicitantes, y la fiabilidad y las garantías de los servicios de certificación que presten.

Desde un punto de vista técnico existen los siguientes tipos de firma:

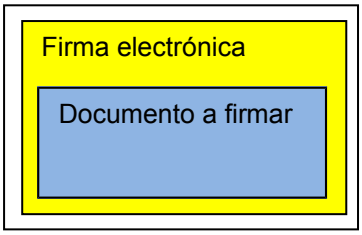
- **Firma attached**: Los datos de firma residen en el documento firmado. Por lo tanto, el mismo documento dispone de toda la información para comprobar la autenticidad e integridad del documento, así como la información necesaria para la validación de la firma. Cabe diferenciar entre dos tipos diferentes de firma attached:
    - **Enveloped** (incrustada), en este caso el documento firmado está compuesto por el contenido del documento a firmar más la firma de este contenido.

Documento firmado:

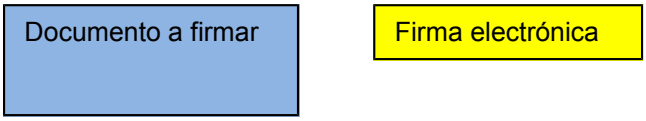


- **Enveloping** (envolvente), en este caso el documento firmado es la firma electrónica del documento a firmar y dentro de esta firma está el propio documento a firmar.

Documento firmado:



- **Firma detached**: los datos de firma residen fuera del documento a firmar, pero asociados a éste. Los datos de la firma se mantendrán por separado durante todo el ciclo de vida del documento. Para validar la firma hay que crear un documento de evidencia electrónica que contenga de forma conjunta el documento y sus datos completos de la firma.

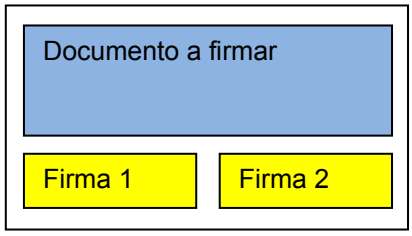


Adicionalmente, sobre un documento podrán realizarse un número variable de firmas electrónicas. En este sentido diferenciaremos entre los siguientes **niveles de firmas**:

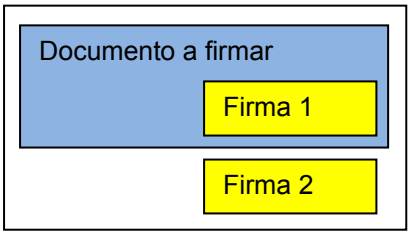
- **Firma simple**: el documento contiene una única firma.
- **Firma múltiple**: el documento contiene dos o más firmas. Esta firma múltiple consiste en que varios firmantes firmen el documento consecutivamente, ya sea de forma secuencial según orden predeterminado o sin que sea relevante el orden las firmas. Este nivel de firma se puede aplicar sobre el documento original cada vez, lo que se

identifica como **firma paralela**, o sobre el documento firmado, que se identifica como **firma anidada**.

Documento firmado con firma paralela:



Documento firmado con firma anidada:



La firma múltiple se utilizará en diversas situaciones en el marco de los procedimientos de la Diputación, como por ejemplo en la firma de documentos electrónicos por más de un empleado público o en el resellado de tiempo de documentos electrónicos firmados previamente (ver apartado anterior) para actualizar la validez legal del documento a lo largo del tiempo, antes de que pueda quedar en entredicho la validez criptográfica de la firma electrónica.

9.1 Formatos de firma.

Partiendo de los conceptos básicos sobre firma electrónica descritos anteriormente, a continuación se describen los formatos de firma electrónica que va a utilizar la Diputación en el marco de esta Política de firma electrónica.

9.1.1 Firma electrónica con política de firma y con sello de tiempo.

Este será el formato de firma electrónica para los documentos electrónicos y foliados de expediente que se deban guardar durante un periodo de tiempo inferior a la caducidad del certificado digital utilizado para generar el sello de

tiempo asociado a la firma electrónica. En el caso de múltiples firmas, se tendrá en cuenta:

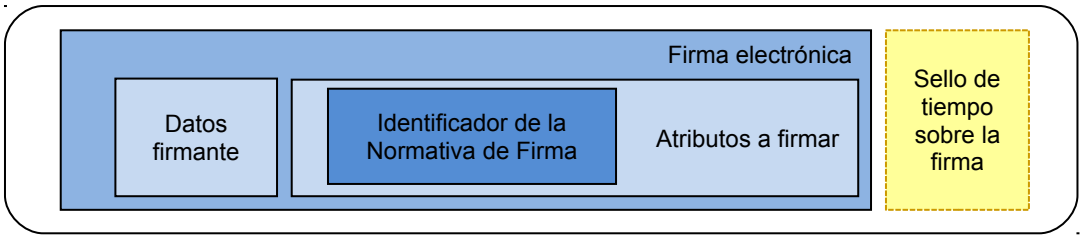
- Firma paralela: la primera fecha de caducidad del sello de tiempo dentro de las distintas firmas.
- Firma anidada: la fecha de caducidad del sello de tiempo de la última firma.

Este formato de firma se genera a partir de:

- Una firma electrónica avanzada que incluye el identificador de la normativa aplicada para generarla. Hasta aquí, técnicamente el formato se conoce como AdES-EPES.
- La incorporación a la anterior de un sello de tiempo que sitúa la firma electrónica en un momento determinado del tiempo. Técnicamente, este formado es conocido como AdES-T.

La representación gráfica de este formato de firma es la siguiente:

Firma electrónica con normativa de firma y sello de tiempo (AdES-T):



La firma electrónica con normativa de firma explícita (AdES-T), debe contener todos los elementos que se listan a continuación de los cuales todos, excepto el último, corresponden al formato AdES-EPES (firma electrónica avanzada con identificador de normativa de firma, pero sin sello de tiempo):

- Los datos firmados por el usuario, como por ejemplo un documento electrónico
- El tipo de contenido firmado: *ContentType*
- El resumen criptográfico del mensaje: *MessageDigest*
- El certificado empleado para firmar: *ESSSigningCertificate* o *OtherSigningCertificate*
- La fecha y hora alegada de la firma: *SigningTime* (Opcional)
- Las pistas sobre el contenido firmado: *ContentHints* (Opcional)
- La identificación del contenido firmado: *ContentIdentifier* (Opcional)
- La referencia a los contenidos: *ContentReference* (Opcional)
- La indicación del tipo de compromiso: *CommitmentTypeIndication* (Opcional)
- La localización del firmante: *SignerLocation* (Opcional)
- Los atributos del firmante: *SignerAttributes* (Opcional)
- El sello de fecha y hora sobre el contenido: *ContentTimestamp* (Opcional)
- Contrafirma: *Countersignature* (Opcional)

- Identificación de la política de firma: *SignaturePolicyIdentifier* (normativa de firma electrónica según esta Política)
- Sello de fecha y hora de la firma: SignatureTimeStamp

9.1.2 Firma electrónica de archivo.

Este será el formato de firma electrónica utilizado para los documentos electrónicos y foliados de expediente que se deban guardar más del tiempo de caducidad del certificado digital utilizado para generar el sello de tiempo asociado a la firma electrónica. En el caso de múltiples firmas, se tendrá en cuenta:

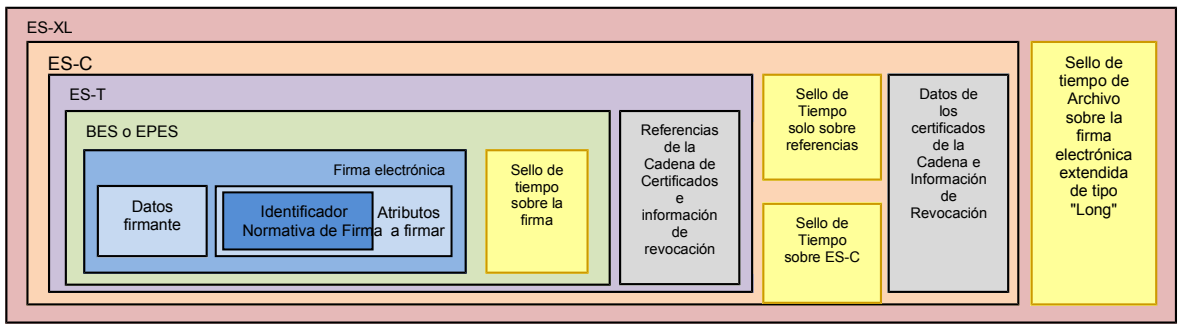
- Firma paralela: la primera fecha de caducidad del sello de tiempo de cada una de las distintas firmas.
- Firma anidada: fecha de caducidad del sello de tiempo de la última firma.

Este formato de firma se genera a partir de:

- Una firma electrónica avanzada extensa que incluye de forma autocontenida todos los elementos de verificación de la vigencia del certificado para poder repetir la validación de la firma de forma autónoma. Hasta aquí, técnicamente el formato se conoce como AdES-XL.
- La incorporación a la anterior de un sello de tiempo que sitúa la firma electrónica en un momento determinado del tiempo, previendo el resellado de tiempo sucesivo de manera periódica para garantir su validez en el tiempo. Técnicamente, este formado es conocido como AdES-A.

El formato AdES-A es el formato de firma más completo y está pensado expresamente para los documentos que se quiere garantizar la disponibilidad y validez a lo largo del tiempo. La representación gráfica de este formato de firma es la siguiente:

Firma electrónica de Archivo (ES-A):



La firma electrónica de archivo (AdES-A), debe contener todos los elementos que se listan a continuación de los cuales todos, excepto el último, corresponden al formato AdES-XL (firma electrónica avanzada con evidencias de validación autocontenidas, pero sin resellado sucesivo de tiempo):

- La firma electrónica: *Signature*
- El certificado utilizado para firmar: *SigningCertificate* o *KeyInfo:X509Data*
- La fecha y hora alegada de la firma: *SigningTime* (Opcional)
- El formato del objeto de datos firmado: *DataObjectFormat* (Opcional)
- La indicación del tipo de compromiso: *CommitmentTypeIndication* (Opcional)
- El lugar de producción de la firma: *SignatureProductionPlace* (Opcional)
- El rol del firmante: *SignerRole* (Opcional)
- El sello de fecha y hora sobre el contenido: *AllDataObjectsTimeStamp* o *IndividualDataObjectsTimeStamp* (Opcional)
- La contrafirma: *Reference* o *CounterSignature* (Opcional)
- Identificación de la política de firma: *SignaturePolicyIdentifier* (normativa de firma electrónica según esta Política)
- Sello de fecha y hora de la firma: *SignatureTimeStamp*
- Referencias completas de certificados: *CompleteCertificateRefs*
- Referencias completas de revocación: *CompleteRevocationRefs*
- Referencias completas de certificados de atributos: *AttributeCertificateRefs*
- Referencias completas de revocación de atributos: *AttributeRevocationRefs*
- Sello de fecha y hora sobre la firma completa: SigAndRefsTimeStamp
- Sello de fecha y hora sobre las referencias de certificados y revocaciones: *RefsOnlyTimeStamp*
- Valores de certificados: *CertificateValues*

- Valores de revocación: *RevocationValues*
- Valores de certificados de atributo: *AttrAuthoritiesCertsValues*
- Valores de revocación de certificados de atributo: *AttributeRevocationValues*
- Sello de fecha y hora de archivo: *ArchiveTimeStamp*

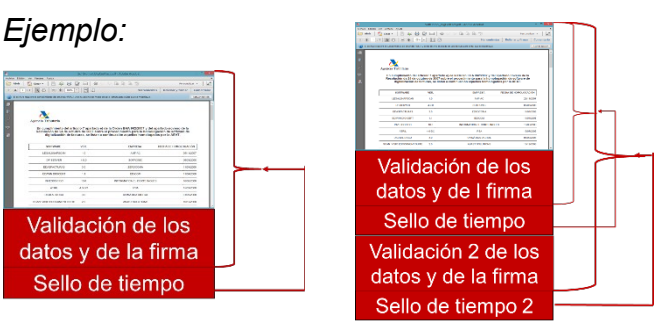
En el caso de firmas sobre documentos con formato PDF este tipo de firma electrónica de archivo se denomina PAdES-LTV o firma electrónica de larga duración (*Long Term Validation*).

Para su generación se parte de una firma AdES-EPES, según hemos visto anteriormente y que sobre documentos PDF se denominará PAdES-EPES incluyendo, de forma recomendada, un sello de tiempo y una respuesta de validación de la firma del servicio OCSP correspondiente. Puede incluir además motivos de firma, el lugar de la firma y datos de contacto del firmante. Incluye además la política de firma.

Sobre estas firmas se puede construir una firma PAdES-LTV que incluye para la verificación de las firmas y del contenido, de que las Autoridades de Certificación en el momento de la validación eran correctas, la respuesta del servicio de validación OCSP y un sello de tiempo sobre esta verificación de firmas.

Se puede añadir a la firma, posteriormente y antes de la caducidad del último sello de tiempo, un nuevo comprobante de verificación que garantiza que la verificación que se hizo en su momento continúa siendo válida y se añade un nuevo sello de tiempo para proteger las firmas y sus validaciones.

Ejemplo:



9.2 Validación de firmas.

Para garantizar la validez jurídica de los documentos electrónicos firmados digitalmente, cualquier documento que entre o se genere en la Diputación y que contenga una firma electrónica y/o un sello de tiempo, previamente a su almacenaje en el gestor documental de la Diputación, será validado convenientemente.

Con el objetivo de validar un documento electrónico firmado electrónicamente o que contenga un sello de tiempo se utilizará la plataforma de validación @firma del Ministerio de Industria, Energía y Turismo y los procedimientos que ésta establezca en cada momento. Sólo en aquellos casos en que el proceso de validación de todas las firmas electrónicas y, en su caso sellos de tiempo, sea satisfactoria se procederá a almacenar el documento electrónico dentro del gestor documental de la Diputación. En caso contrario no se aceptará el documento y se comunicará a su emisor.

En los casos que los documentos firmados electrónicamente provengan de una plataforma de confianza, la cual asegure esta validación, se podrá admitir el documento sin necesidad de volver a validar las firmas electrónicas, como por ejemplo el caso de la plataforma del Estado de facturación electrónica FACe.

En el caso de que sea necesaria la preservación de la validez jurídica del documento más allá del tiempo de vida del certificado digital utilizado para su firma electrónica o del sello de tiempo asociado, se procederá a completar la firma electrónica, en los casos en que ésta aún no lo esté, hasta firma electrónica de archivo, es decir -A o -LTV.

10. MANTENIMIENTO Y PRESERVACIÓN DE FIRMAS ELECTRÓNICAS.

10.1 Resellado de firmas electrónicas.

El objetivo principal de esta función es garantizar la firma electrónica a lo largo del tiempo mediante un proceso consistente en renovar el sello de fecha y hora, añadiendo un nuevo eslabón a la cadena de evidencias electrónicas de la firma electrónica que ya está en el documento.

Para poder aplicar dicho proceso es necesario que las firmas estén en un formato que permita añadir sellos de tiempo sucesivos. Estas son las firmas del tipo AdES-A, XAdES-A en el caso de documentos en formato XML o PAdES-LTV en el caso de documentos en formato PDF. En el caso de que una firma no esté en

estos formatos, previo al resellado se completará la firma, que en cualquier caso estará como mínimo en un formato AdES-T, a uno de los formatos que se acaban de indicar.

Este será un proceso que se realizará:

- En el momento en que esté a punto de caducar el último sello de tiempo aplicado a la firma electrónica a preservar.
- Excepcionalmente, cuando se detecte una posible obsolescencia tecnológica de los algoritmos o de las claves utilizadas para la generación de una firma electrónica.

El proceso de resellado de tiempo de firmas electrónicas partirá, tal y como se acaba de establecer, de documentos firmados de forma longeva con firmas de tipo AdES-A ya que su estructura permite esta posibilidad. Sobre estas firmas se incorporará un nuevo sello de tiempo generado con un certificado digital específico de sellado de tiempo de reciente emisión y, por tanto, que disponga de un período de validez superior al de la firma a resellar, así como de una longitud de clave y algoritmo criptográfico que no estarán comprometidos según es describe en el siguiente subapartado.

En definitiva, el resellado consiste, pues, en mantener la validez de la firma incorporando nueva información criptográfica, concretamente sellos de fecha y hora, en la misma estructura de la firma electrónica.

La Diputación reconoce a través de esta política la existencia de la posibilidad de aplicar medidas de seguridad suficientes que eviten cualquier modificación malintencionada de documentos sin emplear técnicas de resellado de tiempo, asegurando así su integridad y no repudio. Sin embargo, la Diputación opta por el método descrito en este subapartado ya que facilita la disponibilidad de evidencias suficientes de la preservación, reguladas por la Ley 59/2003, de firma electrónica, que de otra manera habría que justificar con un complejo sistema de evidencias electrónicas.

10.2 Mantenimiento de la validez jurídica de las firmas en fase de vigencia.

La firma electrónica otorga validez jurídica a los documentos electrónicos. No obstante, esta validez está sujeta a los siguientes riesgos que deben gestionarse debidamente con tal de mantener la validez jurídica de un documento electrónico

durante las fases de tramitación y vigencia y, en su caso, de archivo. Estos riesgos son:

1. **Caducidad del certificado digital con el que se firma un documento electrónico.** Puede cuestionarse la validez de un documento electrónico a partir del día que caduque el certificado digital que lo firmó, si no se puede acreditar con total garantía la fecha en que se generó dicha firma, la cual debe ser evidentemente posterior a la fecha de emisión del certificado digital y anterior a la fecha de revocación o caducidad del certificado digital. Para garantizar el momento en que se generó la firma electrónica, ésta debe ser completada con un sello de tiempo emitido por una Autoridad de Certificación, siempre antes de la caducidad o revocación del certificado digital que la emitió.

   En aquellas situaciones en que este riesgo pueda materializarse, la Diputación de Castellón realizará firmas como mínimo de formato AdES-T, tanto a nivel de PDFs como de XML.

2. **Validez del certificado digital en el momento de generarse la firma electrónica.** Puede cuestionarse la validez de un documento electrónico si no existe la evidencia suficiente de que el certificado digital estaba vigente el día que se generó la firma electrónica, es decir, no estaba revocado. Para guardar la evidencia de que un certificado digital en una fecha determinada, la de la firma, no estaba revocado es necesario completar la firma con la información de la validación de este aspecto contra la Autoridad de Certificación emisora del certificado en el mismo momento de emisión de la firma.

   En este sentido hay que tener en cuenta que las Autoridades de Certificación, en el momento en que un certificado digital caduca, eliminan las evidencias de revocación de su lista de certificados revocados por lo que si no se guarda la evidencia mencionada, una vez caducado el certificado con el que se emitió la firma electrónica, no existirá la certeza de que el certificado no estaba revocado en el momento de generarla.

   En aquellas situaciones en que este riesgo pueda materializarse, la Diputación de Castellón realizará firmas de formato AdES-XL, tanto a nivel de PDFs como de XML, o superiores, pudiendo ser XAdES-A, en el caso de XML o PAdES-LTV en el caso de PDF.

3. **Obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en el certificado digital y con las que se generan las firmas electrónicas.** Un documento electrónico puede dejar de tener validez jurídica a partir del día en que se ponga en duda la seguridad de las claves criptográficas con las que se firmó. En este escenario podrían reproducirse de forma incontrolada firmas generadas con las claves puestas en duda y, por lo tanto, todas las firmas generadas con la tecnología obsoleta se pondrían en duda. Para resolver este aspecto se requiere de claves criptográficas de mayor longitud y generar sucesivos refirmas a partir de firmas electrónicas que permitan incorporar estos sellos de tiempo.

   En aquellas situaciones en que este riesgo pueda materializarse, igual que en el caso anterior, la Diputación de Castellón realizará firmas de formato AdES-XL, tanto a nivel de PDFs como de XML, o superiores, pudiendo ser XAdES-A, en el caso de XML o PAdES-LTV en el caso de PDF.

Partiendo de la base de lo que se acaba de exponer, la Diputación de Castellón aplicará el siguiente proceso de mantenimiento de la validez jurídica de las firmas electrónicas de aquellos documentos cuya validez jurídica deba ser preservada más allá de la validez del sello de tiempo incorporado a su firma electrónica:

1. Durante la fase de tramitación los documentos generados por la Diputación serán firmados con formatos de firma electrónica preservables, es decir en formato de firma de archivo. En este sentido, todos los documentos a ser firmados serán generados en formato XML, y fima XAdES-A, o PDF/A y firma PAdES-LTV.
2. Para aquellos documentos electrónicos recibidos firmados electrónicamente de terceras partes, una vez validada correctamente la firma, se procederá a completarla hasta convertirla en formato de firma de archivo.

   En este ámbito, se aceptará cualquiera de los formatos de documentos reconocidos por el MGDE de la Diputación de Castellón (ver apartado 3.4.4), pero en caso de diferir de los formatos XML o PDF, y una vez completada la firma del documento recibido hasta un formato preservable, se realizará un proceso de cambio de formato a XML o PDF mediante la emisión de una copia auténtica que será firmada automatizadamente con

sello de órgano de la Diputación. En cualquier caso, el documento de partida se guardará en el formato recibido y con la firma completada.

3. Mientras los documentos residan en el gestor documental, previo al proceso de cierre y foliado del expediente, en el módulo DM de Alfresco, se procederá a su resellado de tiempo periódico siempre con carácter previo a la caducidad del último sello de tiempo asociado a una firma electrónica.

4. En el momento de cierre del expediente y aceptación de su transferencia por parte del Servicio de Archivo, desde el módulo DM al RM de Alfresco, se procederá a realizar el proceso de foliado del expediente por el cual se generará un documento XML con una firma de formato XAdES-A. Este documento contendrá un índice de los documentos que conforman el expediente junto con un resumen criptográfico de los mismos de forma que sólo manteniendo la validez jurídica de la firma electrónica documento de foliado del expediente se garantizará la integridad de los documentos que lo conforman partiendo del recalculo de su resumen criptográfico.

   No obstante, antes del proceso de foliado, se procederá a realizar un proceso de validación de todas las firmas electrónicas asociadas a los documentos que conformarán el foliado del expediente y a completarlas con el resultado de la validación. Ello permitirá garantizar que todos los documentos que conformarán el foliado del expediente al que pertenecen tengan validez jurídica y, por tanto, disponer de una evidencia más de que al cierre del expediente todos los documentos tenían validez jurídica. En caso de error en el proceso de validación la transferencia del expediente bajo la responsabilidad de Archivo será rechazada y no se realizará el proceso de foliado.

5. En el momento de transferencia desde el gestor documental al repositorio de preservación documental o archivo longevo, antes de consolidar el ingreso de los documentos en dicho repositorio, el sistema procederá a validar todas las firmas electrónicas asociadas a los documentos a ingresar, en el caso de expedientes sólo sobre el foliado del expediente, y a completarlas con el resultado de la validación. Ello permitirá garantizar que todo lo que entra en el archivo longevo tenga validez jurídica y, por tanto, disponer de una evidencia más de que al inicio de la preservación los documentos tenían validez jurídica. En caso de error en el proceso de

validación la transferencia del documento al archivo longevo será rechazada.

Por lo tanto, en cualquier caso, se preservarán firmas electrónicas de documentos bajo formato XML o PDF y con tipo de firma XAdES-A o PAdES-LTV, respectivamente.

11. METADATOS DE FIRMA ELECTRÓNICA.

Los metadatos que son de aplicación a las firmas electrónicas que se generen o se reciban en el marco de las actividades de la Diputación de Castellón quedan establecidas por su Modelo de gestión de Documentos Electrónicos en el cual se define el vocabulario de metadatos de la Diputación y que contiene un subconjunto de las mismas de aplicación directa a las firmas electrónicas. Estos metadatos se relacionan a continuación:

Identificador	Metadato	Definición	Consignación
ADPC.3001	Identificador del Firmante	Número de identificación fiscal del firmante. Debe ser extraído del certificado digital.	Obligatorio
ADPC.3002	Tipo de firma	Identificar el tipo de firma. Debe ser extraída de la firma electrónica.	Obligatorio
ADPC.3003	Nombre del Firmante	Nombre de la persona física o jurídica que ha realizado la firma electrónica del documento. Debe ser extraída del certificado digital.	Obligatorio
ADPC.3004	Fecha de firma	Fecha de la generación de la firma. Debe ser extraída de la firma electrónica.	Obligatorio
ADPC.3005	Formato de firma	Formato que tiene la firma. Debe ser extraído de la firma electrónica.	Opcional
ADPC.3005	Cargo del Firmante	Cargo que ocupa el firmante dentro de la organización de la Diputación. Se puede extraer del Directorio Activo de Windows o del portafirmas	Opcional

		en el momento de generarse la firma.	
ADPC.3006	Fecha de Caducidad de la Firma Electrónica	Ante el hecho que, según la Política de Firma de la Diputación, las firmas electrónicas siempre serán de tipo archivo o completadas con un sello de tiempo, este metadato se corresponderá con la fecha de la caducidad del último certificado digital con el que se haya completado con sello de tiempo la firma.	Obligatorio
ADPC.3007	Versión del Vocabulario de Metadatos	Identificador normalizado de la versión del Vocabulario de Metadatos de la Diputación de Castellón según la cual se estructura la descripción de la firma electrónica.	Obligatorio

12. NORMATIVAS DE FIRMA ELECTRÓNICA.

Una normativa de firma electrónica es un documento que contiene un conjunto de normas relativas a la firma electrónica, en un contexto particular (contractual, jurídico, legal,...) que tiene por objetivo poder determinar la validez de una firma electrónica en una transacción en particular.

Estas normas se organizan sobre los conceptos de generación y validación de la firma electrónica y definen las reglas y obligaciones de todos los actores involucrados en estos procesos. En este sentido, especifican la información que debe incluir el firmante en el proceso de generación de la firma, y la información que debe comprobar y complementar el verificador en el proceso de validación de la misma.

La Diputación de Castellón empleará las normativas de firma electrónica compartidas bajo licencia de uso BY-NC-SA de Creative Commons por la empresa Astrea la Infopista Jurídica SL y que se puede consultar de forma actualizada en el siguiente enlace:

http://astrea.es/web12/spcesp.htm

Una vez dentro de este enlace web, para acceder a las normativas de firma electrónica deberá consultarse el apartado 5.1 sobre Estándares técnicos de la Política de Seguridad Documental propuesta por Astrea.

Astrea, con la publicación de la biblioteca de normativas de firma electrónica, pretende facilitar a las herramientas de creación y de validación de firmas electrónicas la automatización de los procesos de tratamiento de las mismas, en base a la normativa de firma electrónica seleccionada en cada caso, mediante el establecimiento de unas reglas básicas, que sean comunes para todas las administraciones públicas. De este modo se homogeneiza el contenido técnico de las firmas electrónicas favoreciéndose así la interoperabilidad de las firmas electrónicas en las relaciones interadministrativas, al.

En este sentido, las diferentes normativas de firma electrónica incorporan compromisos de firma, que son particularizaciones de la política general, y que permiten definir con mayor granularidad los controles sobre las reglas de creación y validación de las firmas electrónicas; como pueden ser: los niveles de seguridad aceptados en el certificado de firma, rol o cargo del responsable de producir la firma, etc.

En la biblioteca de Astrea se recogen las normativas de firma electrónica asociadas a los actos administrativos más relevantes dentro de los procedimientos telemáticos de las administraciones públicas. En total se recogen 34 normativas de firma electrónica según se relacionan a continuación:

- **Acto de ciudadano (5.1.1.1 ETSEAJ)**
    - Acto de declaración de voluntad (5.1.1.2 ETSEAJ)
        - Acto de solicitud de ciudadano (5.1.1.3 ETSEAJ)
        - Acto de conformidad de ciudadano (5.1.1.4 ETSEAJ)

        - Acto negocial de ciudadano (5.1.1.34 ETSEAJ)
    - Acto de comunicación previa de ciudadano (5.1.1.5 ETSEAJ)
    - Acto de declaración responsable de ciudadano (5.1.1.6 ETSEAJ)
    - Acto de queja o sugerencia de ciudadano (5.1.1.33 ETSEAJ)
- **Acto de la Administración (5.1.1.7 ETSEAJ)**
    - Acto administrativo (5.1.1.8 ETSEAJ)
        - Acto resolutorio o de trámite definitivo (5.1.1.9 ETSEAJ)
        - Acto de simple trámite (5.1.1.10 ETSEAJ)
        - Acto de comunicación electrónica (5.1.1.11 ETSEAJ)
            - Acto de recepción electrónica (5.1.1.12 ETSEAJ)
            - Acto de notificación electrónica (5.1.1.13 ETSEAJ)
            - Acto de transmisión electrónica de datos (5.1.1.14 ETSEAJ)
        - Acto de constancia (5.1.1.15 ETSEAJ)
            - Acto de publicación (5.1.1.16 ETSEAJ)
            - Acto de copia auténtica (5.1.1.17 ETSEAJ)
                - Acto de copia auténtica compulsada (5.1.1.18 ETSEAJ)
                - Acto de copia auténtica migrada (5.1.1.19 ETSEAJ)
                - Acto de copia auténtica digitalizada (5.1.1.20 ETSEAJ)
            - Acto de copia simple (5.1.1.21 ETSEAJ)
            - Acto de levantamiento de acta (5.1.1.22 ETSEAJ)
            - Acto certificante (5.1.1.23 ETSEAJ)
        - Acto consultivo (5.1.1.24 ETSEAJ)
        - Acto visto bueno de la Administración (5.1.1.25 ETSEAJ)

- Acto de foliado (5.1.1.26 ETSEAJ)
- Acto de fiscalización (5.1.1.27 ETSEAJ)
- Acto de propuesta (5.1.1.28 ETSEAJ)
- Acto de dación de fe (5.1.1.29 ETSEAJ)
- Acto de solicitud de la Administración (5.1.1.31 ETSEAJ)
- Acto de declaración responsable de la Administración (5.1.1.32 ETSEAJ)

o Acto negocial (5.1.1.30 ETSEAJ)

13. CASOS DE USO DE LA FIRMA ELECTRÓNICA.

13.1 Foliado de expedientes electrónicos.

Previo a la descripción de los casos de uso de firma electrónica que se incluyen en los siguientes subapartados, es interesante comentar un concepto clave en este entorno de la documentación administrativa, y que no es otro que el foliado electrónico del expediente electrónico. Para ello se aprovecha la definición que hace la Ley 11/2007, en su artículo 32:

- El expediente electrónico es el conjunto de documentos electrónicos asociados a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.
- El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Diputación, que garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea necesario, siendo admisible que un mismo documento forme parte de diferentes expedientes electrónicos.

La estructura del foliado del expediente electrónico deberá contener, según el artículo 32.1 de la Ley 11/2007, la lista exhaustiva de todos los documentos que formen parte del expediente guardándose para cada uno de los documentos:

- Clave del catálogo. Consistente en el identificador del documento dentro del expediente y que equivale al metadato con identificador “ADPC_0032” y denominación “Identificador del Documento” según el vocabulario de metadatos de la Diputación.

- Nombre del fichero. Consistente en el metadato con identificador "ADPC_0030" y denominación "Nombre del Documento".
- Resumen criptográfico/"Hash" del documento. Como se ha comentado en el apartado 8.9 de la Política de firma electrónica, esta información permitirá validar la integridad del documento en cualquier momento permitiendo que el documento deje de ser resellado y reduciendo la complejidad tecnológica de las soluciones de preservación de documentos electrónicos de la Diputación. Esto obliga, tal y como se define en el subapartado 3.3.2 del Modelo tecnológico dentro del MGDE, a que exista una funcionalidad que a partir de un documento electrónico calcule el hash de un documento para comprobar su integridad comparándolo con la información que consta en el foliado del expediente al que pertenece.

Finalmente, el índice del contenido del expediente, se guardará en un archivo XML, que deberá estar firmado con sello electrónico de la Diputación. Esta firma será en formato XAdES-A y se aplicarán procedimientos de resellado de tiempo mientras sea necesario preservar el expediente al que pertenece el documento de foliado según la Tabla de Evaluación Documental aplicable.

Cabe mencionar que, en aquellos casos en que la duración del sello de tiempo permita dar cumplimiento a la tabla de evaluación documental de aplicación a la tipología de expediente, podrá emplearse alternativamente el formato de firma XAdES-T al formato XAdES-A y no se requerirá de procesos de resellado de tiempo.

La normativa de firma electrónica que será de aplicación al acto de foliado de expedientes electrónicos es "Acto de foliado (5.1.1.26 ETSEAJ)" bajo el código de referencia 1.3.6.1.4.1.15096.2.3.201104.26.

Después de definir los conceptos de expediente electrónico y de foliado del mismo, se describen los principales casos de uso de la firma electrónica reconocidos por esta Política de firma electrónica i vinculados con la normativa de firma electrónica correspondiente.

13.2 Firma electrónica de un documento electrónico

Este caso de uso reconoce la posibilidad general de firmar electrónicamente documentos en soporte electrónico en cualquier momento de su ciclo de vida independientemente de la aplicación que los genere o los trate. Las principales características de este caso de uso son:

- Se realiza la firma sobre un documento original en soporte electrónico.
- El documento original y las firmas se deben incorporar al sistema de gestión documental.
- Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla y completarla, utilizando los servicios de firma electrónica de la ACCV.
- Hay que incorporar al sistema, la evidencia de validación, es decir, la firma completada, la cual, en el caso de ficheros de formato XML, será el mismo documento con firma attached y, en el caso de ficheros de formato PDF, el mismo documento también con firma attached. Por lo tanto, no se prevé gestionar firmas detached.
- El documento electrónico estará en cualquier formato de los aceptados por la Diputación, pero, en caso de documentos que sea necesario garantizar su preservación a largo plazo, se realizará un proceso previo a la firma electrónica de cambio de formato a PDF/A y XML.
- El documento se podrá firmar diversas veces y por diferentes usuarios.
- Se podrá firmar en paralelo y/o de forma anidada.
- En el caso de documentos que no se deban guardar más allá de la validez del sello de tiempo que utilice la Diputación, la firma se generará en formato AdES-T o si no es posible, se completará hasta a este formato.
- En el caso de que los documentos se deban guardar más allá de la validez del sello de tiempo que utilice la Diputación, la firma electrónica se generará o se completará a AdES-A. Para los documentos PDF será PAdES-LTV y para los documentos XML será XAdES-A.
- El documento resultante será incorporado al gestor documental.

Por lo que respecta al tipo de firma, se establecen las siguientes características o requerimientos:

- Clase de firma: Avanzada o Reconocida.
- Tipo de certificado: Para las firmas generadas por la Diputación, Certificado de trabajador Público o Certificado de Sello Electrónico de la Diputación emitidos por la ACCV. Para las firmas generadas por los ciudadanos,

cualquier certificado digital de los admitidos según esta Política de firma electrónica en el apartado 8.5.1.

- Formatos: PAdES. Inicialmente en formato PAdES-T. En el caso de preservación se completará la firma a formato PAdES-LTV.
- Sello de tiempo: Sí
- Nivel de firma: Simple, Múltiple (anidada o paralelo)
- Tipo de firma: Attached.
- Normativa de firma:
    - En el caso de firma emitida por la Diputación u otra Administración Pública: Acto de la Administración (5.1.1.7 ETSEAJ) bajo el código de referencia 1.3.6.1.4.1.15096.2.3.201104.7
    - En el caso de firma emitida por la ciudadanía: Acto de ciudadano (5.1.1.1 ETSEAJ) bajo el código de referencia 1.3.6.1.4.1.15096.2.3.201104.1

13.3 Copia auténtica electrónica de documentos en papel: digitalización segura.

Este caso de uso reconoce la posibilidad de obtener documentos electrónicos con consideración de copia auténtica a partir de documentos en soporte papel. Las principales características de este caso de uso son:

- Consiste en la firma electrónica de un documento digitalizado, en formato PDF/A, para crear una copia auténtica electrónica.
- La firma es necesaria para garantizar la integridad y la autenticidad del documento digitalizado y la fecha de digitalización.
- El personal de la Diputación que digitaliza la documentación es el responsable de firmar electrónicamente el documento digitalizado, y debe estar habilitado formalmente para hacerlo. Su firma electrónica implicará la exactitud e integridad del documento electrónico obtenido como imagen del documento papel digitalizado
- Los documentos digitalizados se firman incorporando un sello de tiempo. Se genera una firma PAdES-T.

- Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla.
- En el caso de que los documentos se deban guardar más allá de la validez del sello de tiempo que utilice la Diputación, la firma electrónica se generará o se completará a PAdES-LTV.

Por lo que respecta al tipo de firma, se establecen las siguientes características o requerimientos:

- Tipo de firma: Avanzada o Reconocida (sólo en el caso de firma emitida por el trabajador público de la Diputación haciendo uso de tarjeta criptográfica)
- Tipo de certificado: Certificado de trabajador Público o Certificado de Sello Electrónico de la Diputación emitidos por la ACCV.
- Formatos: PAdES. Inicialmente en formato PAdES-T. En el caso de requerirse preservación más allá de la duración del sello de tiempo se completará la firma a formato PAdES-LTV.
- Sello de tiempo: Sí
- Nivel de firma: Simple
- Tipo de firma: Attached.
- Normativa de firma:
    - En el caso de proceso de digitalización asistido por el trabajador público de la Diputación: Acto de copia auténtica compulsada (5.1.1.18 ETSEAJ) bajo el código de referencia 1.3.6.1.4.1.15096.2.3.201104.18
    - En el caso de proceso de digitalización automatizada: Acto de copia auténtica digitalizada (5.1.1.20 ETSEAJ) bajo el código de referencia 1.3.6.1.4.1.15096.2.3.201104.20

13.4 Copia auténtica electrónica de un documento firmado electrónicamente.

Este caso de uso reconoce la posibilidad de obtener copias electrónicas de documentos originales firmados electrónicamente aplicando un cambio de formato a PDF/A para ser entregados al ciudadano o a otras Administraciones Públicas en

soporte electrónico o papel. Las principales características de este caso de uso son:

- A partir de un documento original firmado electrónicamente se obtiene una copia auténtica, firmada digitalmente, para ser entregada al interesado en soporte papel o electrónico.
- La copia del documento electrónico debe estar en un formato normalizado y estandarizado, normalmente PDF, antes de firmarla.
- La copia auténtica del documento electrónico se genera a partir de un proceso por el cual:
    - se eliminan las firmas electrónicas del documento electrónico original origen y se genera el documento PDF con el mismo contenido,
    - se incorpora un Código Seguro de Verificación (CSV) de manera que se pueda imprimir y, posteriormente, mediante este CSV, comprobar en la Sede electrónica de la Diputación la integridad del documento impreso,
    - se incorpora junto el CSV anterior las menciones oportunas para su validación en la Sede electrónica de la Diputación considerándose en cualquier caso la URL en la que se podrá realizar la validación.
    - y, finalmente, se firma de forma automatizada y una única vez con el sello de órgano de la Diputación, según establece la Ley 11/2007 en su artículo 30.5: *"las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas, siempre que incluyan la impresión de un código generado electrónicamente o otros sistemas de verificación que permitan contrastar su autenticidad por medio del acceso a los archivos electrónicos"* de la Diputación y en su artículo 18.1.a): *"Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúne los requisitos exigidos por la legislación de firma electrónica."*

Por lo que respecta al tipo de firma, se establecen las siguientes características o requerimientos:

- Tipo de firma: Avanzada.
- Tipo de certificado: Certificado de Sello Electrónico de la Diputación emitido por la ACCV.
- Formatos: Firma en PDF. Se generará en formato PAdES-T. En el caso de que este documento se deba conservar por un periodo superior a la duración del sello de tiempo, se procederá a completar la firma, creando un PAdES-LTV.
- Sello de tiempo: Sí
- Nivel de firma: Simple
- Tipo de firma: Attached.
- Normativa de firma: Acto de copia auténtica migrada (5.1.1.19 ETSEAJ) bajo el código de referencia 1.3.6.1.4.1.15096.2.3.201104.19

13.5 Procesos de firma automatizada.

Este caso de uso reconoce la posibilidad de firma de varios documentos de forma automática con garantías jurídicas sin requerirse la intervención del firmante en el proceso de firma pudiendo sólo ser realizada con certificados de sello electrónico. Las principales características de este caso de uso son:

- Firma de diversos documentos de forma automática.
- El documento electrónico podrá estar en cualquier formato de los aceptados (PDF y XML).
- Los certificados digitales utilizados para esta finalidad se guardarán de forma segura en el entorno informático que generen los procesos de firma automatizada de manera que sólo éstos procesos puedan hacer uso de ellos.

Los criterios de aplicación y actuación de este caso de uso son:

- Está pensado para aquellas tareas en las que se deben firmar diversos documentos de forma automatizada con garantías jurídicas, como por ejemplo:
    - la digitalización segura automatizada de documentos en soporte papel,

- el resellado de documentos para actualizar su validez criptográfica,
- la generación de documentos de forma automática a partir de la información que constan en los sistemas informáticos de la Diputación como es el caso de certificados de pago de impuestos
- o el intercambio de documentación entre administraciones.

- Se utilizará un certificado de sello electrónico o de órgano, que firmará los documentos en nombre de la aplicación informática y de la Diputación.
- Existirá una evidencia de que el responsable del certificado guardado en los entornos informáticos para la generación de procesos de firma automatizada, la ha autorizado.

Por lo que respecta al tipo de firma, se establecen las siguientes características o requerimientos:

- Tipo de firma: Avanzada.
- Tipo de certificado: Certificado de Sello Electrónico de la Diputación emitido por la ACCV.
- Formatos: Para documentos XML: XAdES-T y para su conservación, XAdES-A. Para documentos PDF: PAdES-T y para su conservación PAdES-LTV.
- Sello de tiempo: Sí
- Nivel de firma: Simple
- Tipo de firma: Attached.
- Normativa de firma: Este es un escenario que se trata de una funcionalidad de soporte a la ejecución de distintas normativas, como pueden ser:
    - Acto de comunicación electrónica (5.1.1.11 ETSEAJ)
        - Acto de recepción electrónica (5.1.1.12 ETSEAJ)
        - Acto de notificación electrónica (5.1.1.13 ETSEAJ)
        - Acto de transmisión electrónica de datos (5.1.1.14 ETSEAJ)
    - Acto de constancia (5.1.1.15 ETSEAJ)

- Acto de publicación (5.1.1.16 ETSEAJ)
- Acto de copia auténtica (5.1.1.17 ETSEAJ)
    - Acto de copia auténtica migrada (5.1.1.19 ETSEAJ)
    - Acto de copia auténtica digitalizada (5.1.1.20 ETSEAJ)
- Acto de levantamiento de acta (5.1.1.22 ETSEAJ)
- Acto certificante (5.1.1.23 ETSEAJ)

- Acto consultivo (5.1.1.24 ETSEAJ)
- Acto visto bueno de la Administración (5.1.1.25 ETSEAJ)
- Acto de foliado (5.1.1.26 ETSEAJ)
- Acto de declaración responsable de la Administración (5.1.1.32 ETSEAJ)

13.5.1 Incorporación de documentos firmados digitalmente y aportados por terceras partes.

Este caso de uso reconoce la posibilidad de que el ciudadano o cualquier otra tercera parte entreguen a la Diputación un documento firmado electrónicamente. En estos casos será necesario:

- Validar las firmas electrónicas del documento.
- En el caso de que las firmas no sean AdES-T o AdES-A/LTV se procederá a completarlas hasta uno de estos tipos en función del tiempo que deba guardarse el documento.
- A continuación se procederá a incorporar al sistema de gestión documental, el documento con sus firmas completadas.
- El documento electrónico recibido estará en cualquier formato de los aceptados por la Diputación, pero, en el caso de documentos que sea necesario preservar a largo plazo se realizarán cambios de formato mediante procedimientos de copia auténtica en PDF o XML con firma AdES-T o AdES-A/LTV, según corresponda. El documento resultante será incorporado al gestor documental.

Por lo que respecta al tipo de firma, se establecen las siguientes características o requerimientos:

- Tipo de firma: Avanzada o Reconocida en función de los certificados utilizados para su firma.
- Tipo de certificado: Cualquier certificado definido en el punto 8.5.1 de esta Política de Firma electrónica.
- Formatos: Para documentos XML: XAdES-T y para su conservación, XAdES-A. Para documentos PDF: PAdES-T y para su conservación PAdES-LTV.
- Sello de tiempo: Aconsejado. Una vez completada la firma: Sí
- Nivel de firma: Simple, Múltiple (anidada o paralelo)
- Tipo de firma: Attached.
- Normativa de firma: todas las normativas consideradas en el ámbito de la normativa Acto de ciudadano (5.1.1.1 ETSEAJ).