Aragonesa de Servicios Telemáticos

ARAGONESA DE SERVICIOS TELEMÁTICOS

Servicio de Firma Electrónica de Gobierno de Aragón

Política de Firma Electrónica

Referencia:	AST-EFIRMA-PoliticaFirmaElectronica.doc
Autor:	AST
Fecha de creación:	01/09/2011
Última actualización:	11/03/2015
Versión:	v1.6
Clasificación:	Público

GOBIERNO DE ARAGON
Departamento de Industria e Innovación

Control del documento

Registro de cambios

Versión	Fecha	Autor	Descripción
V1.0	17/05/2007	Sergio Loras	Creación del documento Inicial
V1.1	17/03/2008	Sergio Loras	Revisión de contenidos
V1.2	16/05/2008	Sergio Loras	Revisión de contenidos
V1.3	15/09/2008	Sergio Loras	Revisión de contenidos
V1.4	01/09/2011	Gestión del Servicio AST	Revisión de contenidos
V1.5	23/10/2014	Mª Eugenia Pamplona	Revisión de contenidos. Certificados y Recomendaciones
V1.6	11/03/2015	Mª Eugenia Pamplona	Revisión de contenidos. Adecuación a política de firma de Administración General del Estado v1.9

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

Contenido

1. CONSIDERACIONES GENERALES 4

1.1. OBJETO DEL DOCUMENTO 4
1.2. ÁMBITO DE APLICACIÓN 4
1.3. REFERENCIAS 4

2. POLÍTICA DE FIRMA ELECTRÓNICA 6

2.1. OBJETIVOS DE UNA FIRMA 6
2.2. FORMATOS ADMITIDOS DE FIRMA 6

2.2.1. Extensión de la firma 6

2.3. USOS DE FIRMA ACONSEJADOS 7

2.3.1. Autenticación ante una aplicación 7
2.3.2. Firma legalmente válida de un documento 7

2.3.2.1. Firma de documento XML 8
2.3.2.2. Firma de documento binario 8
2.3.2.3. Firma de formulario web 8
2.3.2.4. Firma de PDF 8

2.4. ARCHIVADO DE FIRMAS LONGEVAS Y CUSTODIA 9
2.5. REGLAS DE USO DE ALGORITMOS 10

3. POLÍTICA DE VALIDACIÓN DE FIRMA ELECTRÓNICA 12

3.1. PERIODO DE VALIDEZ DE UNA FIRMA 12
3.2. VALIDACIÓN DE UN DOCUMENTO FIRMADO 12
3.3. RESPUESTA DE LA VALIDACIÓN 12

ANEXO I - FORMATOS DE FICHEROS Y OBJETOS BINARIOS ADMITIDOS 14

ANEXO II - CERTIFICADOS USADOS 15

3.4. CERTIFICADO DE SELLO DE ÓRGANO 15
3.5. CERTIFICADO DE SEDE ELECTRÓNICA 15
3.6. CERTIFICADO DE EMPLEADO PÚBLICO 15
3.7. CERTIFICADO DE PERSONA FÍSICA Y PERSONA JURÍDICA 15
3.8. CERTIFICADO DE FIRMA DE CÓDIGO 16

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

1. Consideraciones Generales

1.1. Objeto del documento

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.

La política de firma electrónica y certificados de Gobierno de Aragón tiene por objeto establecer una serie de recomendaciones comunes para los desarrolladores de aplicaciones de firma electrónica, basadas en el Reglamento Europeo 910/2014, las normativas vigentes a nivel estatal y autonómico, y diferentes documentos del European Telecommunications Standards Institute / Electronic Signatures and Infrastructures (ETSI/ESI).

1.2. Ámbito de aplicación

Este documento especifica las condiciones generales aplicables a la firma electrónica para su validación, en la relación electrónica de la Diputación General de Aragón (DGA), y sus organismos públicos vinculados o dependientes con los ciudadanos y en los órganos y entidades de DGA así como sus organismos vinculados o dependientes.

1.3. Referencias

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

- ETSI TS 101 733, v.1.6.3 Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 101 903, v.1.2.2. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).
- IETF RFC 2630, RFC 3369 y RFC 3852, Cryptographic Message Syntax (CMS).
- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP

Igualmente, se ha considerado como normativa básica aplicable a la materia:

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- 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.
- Reglamento (UE) Nº910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

2. Política de Firma Electrónica

2.1. Objetivos de una firma

Podemos distinguir dos objetivos:

- **Autenticación ante una aplicación**. Cuando queremos usar un mecanismo de autenticación fuerte como es el basado en firma electrónica para asegurar la identidad del usuario.
- **Firma legalmente valida de un documento**. Cuando queremos que un documento electrónico firmado tenga la misma validez que un documento con firma manuscrita.

2.2. Formatos admitidos de firma

Para asegurar los periodos de validez y objetivos de una firma electrónica, actualmente se consideran formatos admitidos:

- **Formato XAdES** (XML Advanced Electronic Signatures) según especificación ETSI TS 101 903, versión 1.2.2
- **Formato CAdES** (CMS Advanced Electronic Signatures) según especificación ETSI TS 101 733, versión 1.6.3 y versión 1.7.

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.

En el momento de la firma se deberá incluir la referencia del identificador único de la versión del documento de política de firma electrónica sobre el que se ha basado su implementación, el cual determinará las condiciones que debe cumplir la firma electrónica en un momento determinado.

El campo destinado para incluir esta referencia será, sólo para el formato AdES_EPES, la etiqueta SignaturePolicyIdentifier.

2.2.1. Extensión de la firma

Se recomienda que el fichero resultante de firma tenga una extensión única de forma que los visores de documentos firmados puedan asociarse a una extensión, haciendo más fácil al usuario el manejo de este tipo de ficheros. Esta extensión podría ser:

- **.xsig**, si la firma implementada se ha realizado según los estándares XAdES o XMLDSig
- **.csig** si la firma implementada se ha realizado según los estándares CAdES o CMS.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

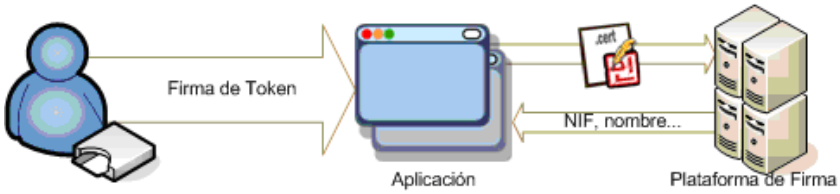
2.3. Reglas de usos de firma

Desde Aragonesa de Servicios Telemáticos se aconsejan estos usos y tipos de firma para los siguientes casos. En cualquier caso, habría que valorar más a fondo los factores que puedan afectar a cada procedimiento para acabar decantándose por un uso o tipo de firma.

Para todos los procedimientos expuestos a continuación, se debe contemplar que tienen que permitir el uso de todos los certificados emitidos por las autoridades de certificación con las que el Gobierno de Aragón ha llegado a convenio para reconocerlas.

2.3.1. Autenticación ante una aplicación

Para este objetivo, desde Aragonesa de Servicios Telemáticos se recomienda implementar un mecanismo de firma, para asegurarnos que el usuario es poseedor de la clave privada asociada al certificado con el que se quiere autenticar, razón por la que no basta con validar el certificado de clave pública.



Al implementar un mecanismo de firma, por ser ésta de corta duración y su único objetivo el de autenticar al firmante ante la aplicación, bastará con una firma **CAdES-BES** o **CAdES-EPES**. Se firmará un token aleatorio que se validará en el servidor, y si la firma es correcta se procederá a acceder a los atributos del certificado que interesen para evaluar si se debe o no dar acceso a la aplicación.

Es muy importante distinguir el proceso de autenticación con el de firma de documentos, y que aunque pertenezcan a la misma persona el certificado usado para autenticarse puede ser diferente al usado para firmar un documento una vez dentro de la aplicación (Por ejemplo, es el caso del uso del DNI Electrónico).

2.3.2. Firma legalmente válida de un documento

A la hora de que una aplicación ofrezca al usuario la posibilidad de firmar un documento, hay una serie de requisitos que se deben cumplir para considerar el proceso válido.

- La comunicación debe estar securizada usando el protocolo HTTPS.
- Los algoritmos usados para realizar la firma deben ser seguros y no mostrar ninguna vulnerabilidad, por lo que estos deben ser configurables dentro de la aplicación, para posibles cambios en el futuro.
- El firmante tiene que poder visualizar los datos a firmar.
- El certificado del firmante tiene que ser uno de los emitidos por las Autoridades de Certificación reconocidas por Gobierno de Aragón.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

- Opcionalmente se pueden solicitar algunos datos al firmante como:
  - Política de firma empleada.
  - Rol del firmante.
  - Acción del firmante (Ej: lo aprueba, lo informa, lo recibe, lo certifica, etc.)
  - Localización de la firma.
  - Formato del documento original.

Una vez concluido el proceso de firma, automáticamente se desencadenará el proceso de validación de la misma para actualizar su nivel si es necesario.

2.3.2.1. Firma de documento XML

En los casos que queramos firmar un documento XML, la firma que debe realizar el usuario será inicialmente una **XAdES-BES** o **XAdES-EPES attached enveloping** o **enveloped**. En el caso de que no firmemos todo el XML, sino unos nodos en concreto, el formato será enveloped obligatoriamente.

Una vez tengamos esa firma deberemos actualizara hasta un nivel que satisfaga las necesidades de su tiempo de vida estimado. Como mínimo la firma se actualizará hasta un nivel **XAdES-T**, para permitirnos situar en el tiempo el momento de la firma.

2.3.2.2. Firma de documento binario

Al ser un documento binario y para no modificarlo, usaremos firmas **CAdES detached**, siendo su actualización respecto a su tiempo de vida estimado, el análogo al de la firma de un documento XML.

2.3.2.3. Firma de formulario web

Para este caso, lo aconsejable es transformar el formulario web a un documento XML con las herramientas oportunas y seguir las recomendaciones para la firma de un documento XML.

2.3.2.4. Firma de PDF

Aunque existen firmas PDF, que pueden integrarse en el propio documento PDF y ser reconocidas por Adobe Reader y verificadas por él, éstas, al no ser firmas avanzadas (son firmas **CMS detached** incrustadas dentro del PDF) y por lo tanto, no aseguran su perdurabilidad a lo largo del tiempo, por lo que no son recomendadas desde AST.

Es recomendado entonces seguir los mismos pasos de firma para un documento binario cualquiera.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

2.4. Archivado de firmas longevas 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 o CAdES, 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 **AdES-A**. Este nivel está preparado para ir guardando sellos de tiempo sucesivos que nos aseguren la validez de la firma hasta que creamos conveniente.

- 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 CAdES o XAdES:

- Las plataformas de firma electrónica adoptadas en el ámbito de la DGA deberán disponer de mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente. Este proceso debe ser lanzado manualmente dado el caso.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

- 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.

Una aplicación debe encargarse de resellar sus documentos firmados antes de que caduque el último sello de tiempo, es decir antes de la fecha marcada por el campo **Valido hasta** del certificado de la Autoridad del Sellado de Tiempo. Este proceso puede ser automático, ya que se sabe de antemano la fecha de caducidad del certificado de la TSA.

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).

2.5. 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 y CAdES, 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/SHA256 y RSA/SHA512 que es recomendado para archivado de documentos electrónicos (very long term signatures).

Al no ser visible la firma electrónica, será necesario incluir a la hora de imprimir el documento los datos necesarios para que la firma quede reflejada:

- Nombre del firmante
- Emisor del certificado del firmante
- Fecha de la firma
- Código de verificación

Un código de verificación permite acceder al documento electrónico original a partir de la copia en papel. Este código en papel puede consistir en varias soluciones:

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

- Una URL donde encontrar accesible el documento.
- Un ID a partir del cual poder acceder al documento dentro de la aplicación.
- Un código de barras PDF-417 que permita serializar el documento original firmado.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

3. Política de Validación de Firma Electrónica

3.1. Periodo de validez de una firma

Podemos distinguir dos casos:

- **Firmas de corta duración**: firmas que no necesitan ser validadas después de que expire la validez del certificado del firmante. Una vez que el certificado del firmante esté caducado o revocado, esta firma perderá toda validez legal.

- **Firmas de larga duración**: firmas que van a tener que ser verificadas posiblemente después de que el certificado del firmante haya expirado, incluso después de que el certificado del emisor del certificado haya expirado. Para ello se recurren a métodos como los sellos de tiempo y a la preservación de los métodos de revocación para prolongar la validez de la firma.

3.2. Validación de un documento firmado

En este proceso se determinará si la firma es valida o no, y debe realizarse por primera vez, acto seguido de generar la firma, para ello serán obligatoriamente necesarios los siguientes elementos:

- El documento. En el caso de que se desee comprobar la integridad del mismo.

- La firma electrónica.

3.3. Respuesta de la validación

De la respuesta de una validación se obtienen principalmente dos elementos que la aplicación deberá evaluar:

- **Estado de la validación**.

  - Validación completada, donde todo el proceso de validación es considerado completado y se puede asegurar un resultado.

  - Validación fallida**,** donde dependiendo de varios factores la validación no puede ser considerada completa.

- **La propia firma**, que ha podido ser actualizada en los siguientes casos:

  - En caso de que asi se haya establecido en la aplicación para obtener el nivel de firma AdES necesario.

  - Si un sello de tiempo está a punto de caducarse, un sello de tiempo adicional debe ser añadido para prolongar la vida de la firma si es necesario.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

- Si la tecnología que se usó ahora es vulnerable, o lo será en breves, información adicional debe ser añadida para asegurar la validez de la firma.

La aplicación debé mostar al usuario la siguiente información en una validación de un documento firmado:

- El documento del firmante en el formato original en la que se firmo, si por alguna razón, el contenido del documento no puede ser visualizado exactamente de la forma en la que se firmo, se debe informar claramente.
- El estado de la firma.
- DN del certificado del firmante.
- DN del certificado de la autoridad de certificación que ha emitido el certificado.
- DN de las autoridades de certificación de la cadena de confianza hasta el nivel marcado por la aplicación.
- La fecha de la firma.

Usando el correspondiente interface, el usuario debe encontrar la siguiente información adicional:

- Otro contenido del certificado del firmante (Nombre, apellidos, NIF, correo…).
- El formato del documento que fue firmado.
- El lugar de la firma, si estuviese disponible.
- La política de firma usada, si estuviese disponible.
- La acción del firmante, si estuviese disponible.
- Roles del certificado usados en al firma, si estuviesen disponibles.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

Anexo I - Formatos de ficheros y objetos binarios admitidos

Este marco de condiciones generales sobre los formatos de fichero de referencia a admitir por las plataformas de relación electrónica de la DGA con los ciudadanos y con las Administraciones Públicas pretende establecer unas consideraciones generales así como la relación de formatos de fichero y objetos binarios que deberán ser admitidos por todas las plataformas para facilitar su interoperabilidad. No obstante lo anterior, estas plataformas podrán admitir otros formatos de acuerdo con las necesidades específicas que en cada caso se planteen.

La relación completa de las condiciones generales en materia de formatos de fichero se establecerá por el marco normativo de desarrollo del Esquema Nacional de Interoperabilidad tal y como estable la Disposición adicional primera del Real Decreto 4/2010, de 8 de enero.

- 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 auto-contenidos. 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.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

Anexo II - Certificados usados

Los certificados son los encargados de autenticar al firmante, mediante la relación que crea entre su identidad y las claves usadas en el proceso de firma.

La Ley 11/2007 para el Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) marca una serie de mecanismos para la relación entre Administraciones Públicas, ciudadanos y empresas, para ello hay que contemplar los distintos tipos de certificados que se pueden usar en estos mecanismos.

3.4. Certificado de sello de órgano

Este tipo de certificados serán empleados por el Gobierno de Aragón y sus departamentos para identificarse como organismo en los documentos que se produzcan desde la Administración.

Actualmente Gobierno de Aragón utiliza para este fin la Autoridad de Certificación FNMT-RCM SubCA Componentes Informáticos

3.5. Certificado de sede electrónica

Será el empleado por los sitios web del Gobierno de Aragón y sus departamentos para autenticarse y ofrecer un canal de comunicación seguro. Estos certificados no podrán usarse para generar firmas, solo exclusivamente para autenticar sitios web.

Actualmente se usan para este fin los certificados de servidor de la Autoridad de Certificación FNMT Clase AP.

3.6. Certificado de empleado público

Actualmente todo empleado público de Gobierno de Aragón puede disponer de una tarjeta criptográfica donde se incorpore su certificado de personal como persona física emitido por FNMT Clase 2 CA, y opcionalmente también puede hacer uso del DNI Electrónico como marca la LAECSP.

Es importante reflejar que a pesar del uso de estos certificados para este fin, en ninguno de estos certificados queda reflejada la vinculación entre el propietario del certificado y el Gobierno de Aragón teniendo que usar otros medios para reflejar esa relación como se comenta en el artículo 19 de la LAECSP.

3.7. Certificado de persona física y persona jurídica

Serán los empleados por ciudadanos y empresas para identificarse ante las aplicaciones del Gobierno de Aragón. Los más comunes serán los emitidos por FNMT y Dirección General de Policía, pero estos certificados podrán ser cualquiera de los emitidos por las Autoridades de Certificación Autorizadas por Gobierno de Aragón.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es

3.8. Certificado de firma de código

Será el empleado por Aragonesa de Servicios Telemáticos, como entidad proveedora de los productos software del Gobierno de Aragón, para firmar los componentes informáticos (Applets Java, librerías DLL, …) que así lo requieran para cumplir los niveles de seguridad adecuados.

Actualmente se usa para este fin un certificado de firma de código emitido por FNMT-RCM AC Componentes Informáticos.

Entidad Pública Aragonesa de Servicios Telemáticos
Av Pablo Ruiz Picasso, 63 A 3ª J • 50018 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4145
www.aragon.es