DECISIONES

DECISIÓN DE LA COMISIÓN

de 25 de febrero de 2011

por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior

[notificada con el número C(2011) 1081]

(Texto pertinente a efectos del EEE)

(2011/130/UE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior [1], y, en particular, su artículo 8, apartado 3,

Considerando lo siguiente:

(1) Los prestadores de servicios cuyos servicios entren en el ámbito de aplicación de la Directiva 2006/123/CE deben poder llevar a cabo a través de ventanillas únicas y por vía electrónica los procedimientos y trámites necesarios para acceder a sus actividades y ejercerlas. Dentro de los límites establecidos en el artículo 5, apartado 3, de la Directiva 2006/123/CE, puede darse aún el caso de que los prestadores de servicios tengan que presentar documentos originales, copias compulsadas o traducciones compulsadas cuando efectúen dichos procedimientos y trámites. En estos casos, es posible que los prestadores de servicios tengan que presentar documentos firmados electrónicamente por autoridades competentes.

(2) La utilización transfronteriza de las firmas electrónicas avanzadas basadas en un certificado reconocido queda facilitada en virtud de la Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior [2], que, entre otras cosas, obliga a los Estados miembros a llevar a cabo una evaluación de los riesgos antes de exigir estas firmas electrónicas a los prestadores de servicios y establece unas normas para la aceptación por los Estados miembros de las firmas electrónicas avanzadas basadas en certificados reconocidos, con o sin dispositivo seguro de creación de firma. No obstante, la Decisión 2009/767/CE no entra en los formatos de las firmas electrónicas en los documentos expedidos por las autoridades competentes que los prestadores de servicios deben presentar cuando lleven a cabo los procedimientos y trámites pertinentes.

(3) Dado que las autoridades competentes de los Estados miembros utilizan actualmente diferentes formatos de firma electrónica avanzada para firmar electrónicamente sus documentos, los Estados miembros receptores que tienen que procesar dichos documentos pueden encontrar dificultades técnicas derivadas de la variedad de formatos de firma utilizados. Para que los prestadores de servicios puedan llevar a cabo sus procedimientos y trámites por vía electrónica a través de las fronteras, es necesario garantizar que los Estados miembros puedan dar soporte técnico al menos a cierto número de formatos de firma electrónica avanzada cuando reciban documentos firmados electrónicamente por autoridades competentes de otros Estados miembros. La definición de cierto número de formatos de firma electrónica avanzada a los que tendría que dar soporte técnico un Estado miembro receptor facilitaría la automatización y mejoraría la interoperabilidad transfronteriza de los procedimientos electrónicos.

(4) Es posible que los Estados miembros cuyas autoridades competentes utilicen formatos de firma electrónica distintos de los comúnmente aceptados hayan implementado medios de validación que permitan verificar sus firmas también más allá de sus fronteras. Cuando tal sea el caso, y a fin de que los Estados miembros receptores puedan utilizar estas herramientas de validación, es necesario que la información sobre ellas esté disponible y sea de fácil acceso, a menos que la información necesaria vaya incluida directamente en los documentos electrónicos, en las firmas electrónicas o en los portadores de los documentos electrónicos.

(5) La presente Decisión no afecta a la determinación por parte de los Estados miembros de qué constituye un original, una copia compulsada o una traducción compulsada. Su objetivo se limita a facilitar la verificación de las firmas electrónicas usadas en los originales, copias compulsadas o traducciones compulsadas que los prestadores de servicios puedan tener que presentar a través de las ventanillas únicas.

[1] DO L 376 de 27.12.2006, p. 36.
[2] DO L 274 de 20.10.2009, p. 36.

(6) A fin de permitir a los Estados miembros que implementen las herramientas técnicas necesarias, conviene que la presente Decisión sea aplicable a partir del 1 de agosto de 2011.

(7) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité de la Directiva de servicios.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Formato de referencia para las firmas electrónicas

1. Los Estados miembros implantarán los medios técnicos necesarios para procesar los documentos firmados electrónicamente por las autoridades competentes de otros Estados miembros con una firma electrónica avanzada XML o CMS o PDF, en formato BES o EPES, que se ajuste a las especificaciones técnicas contenidas en el anexo, que presenten los prestadores de servicios en el contexto del cumplimiento de los procedimientos y trámites a través de las ventanillas únicas, según lo previsto en el artículo 8 de la Directiva 2006/123/CE.

2. Los Estados miembros cuyas autoridades competentes firmen los documentos a que se refiere el apartado 1 utilizando otros formatos de firma electrónica distintos de los mencionados en dicho apartado deberán notificar a la Comisión las posibilidades de validación existentes para que otros Estados miembros puedan validar en línea, gratuitamente y sin que sea necesario conocer la lengua original, las firmas electrónicas recibidas, a menos que la información requerida vaya incluida en el documento, en la firma electrónica o en el portador del documento electrónico. La Comisión pondrá dicha información a disposición de todos los Estados miembros.

Artículo 2

Aplicación

La presente Decisión se aplicará a partir del 1 de agosto de 2011.

Artículo 3

Destinatarios

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 25 de febrero de 2011.

Por la Comisión

Michel BARNIER

Miembro de la Comisión

ANEXO

Especificaciones para que una firma electrónica avanzada XML, CMS o PDF sea soportada técnicamente por el Estado miembro receptor

En la siguiente parte del documento, las palabras clave «DEBERÁ» (MUST), «NO DEBERÁ» (MUST NOT), «OBLIGATORIO» (REQUIRED), el «tiempo futuro» (SHALL), el «tiempo futuro negativo» (SHALL NOT), «DEBERÍA» (SHOULD), «NO DEBERÍA» (SHOULD NOT), «RECOMENDADO» (RECOMMENDED), «PODRÁ» (MAY), y «OPCIONAL» (OPTIONAL), o sus variantes gramaticales, deberán interpretarse de acuerdo con lo descrito para sus equivalentes en lengua inglesa en el documento RFC 2119 ([1]).

SECCIÓN 1 – XAdES-BES/EPES

La firma se ajusta a las especificaciones del W3C para la firma XML ([2]).

La firma DEBERÁ ser al menos una forma de firma XAdES-BES (o -EPES) según se especifica en las especificaciones ETSI TS 101 903 XAdES ([3]) y ajustarse a todas las especificaciones adicionales siguientes:

El ds:CanonicalizationMethod que especifica el algoritmo de canonicalización aplicado al elemento SignedInfo antes de llevar a cabo los cálculos de la firma designa solamente uno de los siguientes algoritmos:

Canonical XML 1.0 (omits comments):	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Canonical XML 1.1 (omits comments):	http://www.w3.org/2006/12/xml-c14n11
Exclusive XML Canonicalization 1.0 (omits comments):	http://www.w3.org/2001/10/xml-exc-c14n#

NO DEBERÍAN utilizarse para la creación de firmas otros algoritmos ni tampoco versiones «with comments» de los mencionados, pero sí DEBERÍAN soportarse para la interoperabilidad residual a efectos de la verificación de firmas.

NO DEBERÁ utilizarse MD5 (RFC 1321) como algoritmo de compendio. Se remite a los firmantes a la legislación nacional aplicable y, a efectos de directrices, a ETSI TS 102 176 ([4]) y al informe ECRYPT2 D.SPA.x ([5]) para más recomendaciones sobre algoritmos y parámetros utilizables en firmas electrónicas.

Se restringe el uso de *transformaciones* a las enumeradas a continuación:

transformaciones de canonicalización: véanse las especificaciones conexas citadas anteriormente;

codificación en base64 (http://www.w3.org/2000/09/xmldsig#base64);

filtrado:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): por razones de compatibilidad y conformidad con XMLDSig,

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): como sucesor de XPath por cuestiones de rendimiento;

transformación de firma envuelta: (http://www.w3.org/2000/09/xmldsig#enveloped-signature);

transformación XSLT (hoja de estilos).

El elemento ds:KeyInfo DEBERÁ incluir el certificado digital X.509 v3 del firmante (es decir, su valor, y no solo una referencia a él).

La propiedad firmada de la firma SigningCertificate DEBERÁ contener el valor de compendio (CertDigest) y el IssuerSerial del certificado del firmante almacenado en ds:KeyInfo y NO DEBERÁ utilizarse el URI opcional del campo SigningCertificate.

La propiedad firmada de la firma SigningTime está presente y contiene el UTC expresado como xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

El elemento DataObjectFormat DEBERÁ estar presente y contener el subelemento MimeType.

En caso de que las firmas utilizadas por los Estados miembros se basen en un certificado reconocido, los objetos PKI (cadenas de certificados, datos de revocación, sellos temporales) incluidos en las firmas se pueden verificar utilizando la Lista de Confianza, de conformidad con la Decisión 2009/767/CE de la Comisión, del Estado miembro que supervisa o acredita al PSC que ha expedido el certificado del signatario.

El cuadro 1 resume las especificaciones a que debe ajustarse una firma XAdES-BES/EPES para ser soportada técnicamente por el Estado miembro receptor.

([1]) IETF RFC 2119: «Key words for use in RFCs to indicate Requirements Levels».
([2]) W3C, XML Signature Syntax and Processing, (Version 1.1), http://www.w3.org/TR/xmldsig-core1/.
W3C, XML Signature Syntax and Processing, (Second Edition), http://www.w3.org/TR/xmldsig-core/
W3C, XML Signature Best Practices, http://www.w3.org/TR/xmldsig-bestpractices/.
([3]) ETSI TS 101 903 v1.4.1: XML Advanced Electronic Signatures (XAdES).
([4]) ETSI TS 102 176: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; Part 2: «Secure channel protocols and algorithms for signature creation devices».
([5]) La versión más reciente es D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), de fecha 30 de marzo de 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Cuadro 1

XAdES - BES (EPES)		**Requisitos mínimos comunes**
(ETSI TS 103 903 applies with the following profiled elements)		
O=obligatorio; F=facultativo; R=recomendado; N=no se usa		
ds: Signature ID	O	
ds: SignedInfo	O	
ds: CanonicalizationMethod	O	*DEBERÁN soportarse para la verificación de firmas todos los algoritmos siguientes, la creación DEBERÍA restringhirse a uno de estos:* *- Exclusive XML canonicalization 1.0: http://www.w3.org/TR/xml-exc-c14n/* *- Canonical XML 1.0: http://www.w3.org/TR/2001/REC-XML-c14n-20010315* *- Canonical XML 1.1: http://www.w3.org/2006/12/xml-c14n11* *NO DEBERÍAN usarse otros métodos ni versiones "#WithComments" de los anteriores.*
ds: SignatureMethod	O	***Algoritmos:*** *remitirse a la legislación nacional aplicable y, a efectos de directrices, a ETSI TS 102 176 y al informe ECRYPT2 D.SPA.7 para más recomendaciones.*
ds: Reference URI	O	Una referencia a cada objeto de datos original que debe firmarse (los URI pueden apuntar también a objetos externos), + referencia al elemento SignedProperties
ds: Transforms	F	*Las aplicaciones de verificación DEBERÁ soportar todas las transformaciones siguientes, mientras que la aplicación de creación de firmas DEBERÍA restringir el uso de transformaciones a las siguientes:* *- transformaciones de canonicalización: véase más arriba* *- codificación en Base64* *- XPath y XPath Filter 2.0* *- transformación de firma envuelta* *- transformaciones XSLT*
ds: DigestMethod	O	*Algoritmos: remitirse a la legislación nacional aplicable y, a efectos de directrices, a ETSI TS 102 176 y al informe ECRYPT2 D.SPA.7 para más recomendaciones.*
ds: DigestValue	O	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	O	
ds: KeyInfo	O	DEBERÁ contener el certificado X509 (la propiedad firmada SigningCertificate DEBERÁ contener el valor de compendio del certificado de este firmante) SE RECOMIENDA aportar la cadena de certificación del certificado del firmante como ayuda para facilitar el proceso de validación (en este caso DEBERÁN aportarse los certificados X.509).
ds: Object		
QualifyingProperties	O	
SignedProperties	O	O
SignedSignatureProperties	O	O
SigningTime	O	UTC (xsd: dateTime).
SigningCertificate	O	DEBERÁ contener el valor de compendio del certificado del firmante almacenado en ds:KeyInfo con omisión del URI opcional (las aplicaciones PODRÁN buscar/encontrar el certificado del firmante en ds:KeyInfo sobre la base de la equivalencia hash).
SignaturePolicyIdentifier	F	solo para la forma EPES (y formas superiores construidas a partir de la forma EPES)
Signature ProductionPlace	F	
SignerRole	F	
/SignedSignatureProperties		
SignedDataObjectProperties	F	
DataObjectFormat	O	Cuando se use este campo, las aplicaciones GARANTIZARÁN que los objetos de datos se muestran al usuario en consonancia con ello. Si se usa, DEBERÁ utilizarse un elemento hijo MimeType.
CommitmentTypeIndication	F	
AllDataObjectsTimeStamp	F	
IndividualDataObjectTimeStamp	F	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	F	
UnsignedSignatureProperties		
CounterSignature	F	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		

SECCIÓN 2 – CAdES-BES/EPES:

La firma se ajusta a las especificaciones de la Cryptographic Message Syntax (CMS) ([1]).

La firma utiliza los atributos de firma CAdES-BES (o -EPES) según se especifican en las especificaciones ETSI TS 101 733 CAdES ([2]) y se ajusta a las especificaciones adicionales indicadas en el cuadro 2.

Todos los atributos de CAdES que están incluidos en el cálculo hash del sello temporal del archivo (ETSI TS 101 733 V1.8.1 Annex K) DEBERÁN estar codificados con DER y cualquier otro puede estarlo con BER para simplificar el procesamiento CAdES en una sola pasada.

NO DEBERÁ utilizarse MD5 (RFC 1321) como algoritmo de compendio. Se remite a los firmantes a la legislación nacional aplicable y, a efectos de directrices, a ETSI TS 102 176 ([3]) y al informe ECRYPT2 D.SPA.x ([4]) para más recomendaciones sobre algoritmos y parámetros utilizables en firmas electrónicas.

Los atributos firmados DEBERÁN incluir una referencia al certificado digital X.509 v3 (RFC 5035) del firmante y el campo *SignedData.certificates* DEBERÁ incluir su valor.

El atributo firmado SigningTime DEBERÁ estar presente y DEBERÁ contener el UTC expresado con arreglo a http://tools.ietf.org/html/rfc5652#section-11.3.

El atributo firmado ContentType DEBERÁ estar presente y contener datos de identificación (http://tools.ietf.org/html/rfc5652#section-4), donde el tipo de contenido de datos se refiere a cadenas de octetos arbitrarias, tales como texto UTF-8 o contenedor ZIP con subelemento MimeType.

En caso de que las firmas utilizadas por los Estados miembros se basen en un certificado reconocido, los objetos PKI (cadenas de certificados, datos de revocación, sellos temporales) incluidos en las firmas se pueden verificar utilizando la Lista de Confianza, de conformidad con la Decisión 2009/767/CE de la Comisión, del Estado miembro que supervisa o acredita al PSC que ha expedido el certificado del signatario.

([1]) IETF, RFC 5652, Cryptographic Message Syntax (CMS), http://tools.ietf.org/html/rfc5652.
IETF, RFC 5035, Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility, http://tools.ietf.org/html/rfc5035.
IETF, RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), http://tools.ietf.org/html/rfc3161.

([2]) ETSI TS 101 733 v.1.8.1: CMS Advanced Electronic Signatures (CAdES).

([3]) ETSI TS 102 176: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; Part 2: «Secure channel protocols and algorithms for signature creation devices».

([4]) La versión más reciente es D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), de fecha 30 de marzo de 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Cuadro 2

CAdES - BES (EPES)		**Requisitos mínimos comunes**
(ETSI TS 103 903 applies with the following profiled elements)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
O=obligatorio; F=facultativo; R=recomendado; N=no se usa		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	O	**Algoritmos:** remitirse a la legislación nacional aplicable y, a efectos de directrices, a ETSI TS 102 176 y al informe ECRYPT2 D.SPA.7 para más recomendaciones.
encapContentInfo SEQUENCE {		
eContentType ContentType,	O	id-Data
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	O/N	El atributo firmado ContentType está presente y contiene datos de identificación (http://tools.ietf.org/html/rfc5652#section-4) donde el tipo de contenido de datos se refiere a cadenas arbitrarias de octetos, tales como texto UTF-8 o contenedor ZIP con subelemento MimeType
-- External Data (if signature detached)*		si no está presente de otra manera la firma separada. * Son datos externos los datos protegidos por una firma separada no incluida en el eContent de la firma CAdES. Se recomienda incluir los datos externos firmados junto con la firma en un archivo ZIP.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	O	DEBERÁ contener el certificado X509 del firmante. SE RECOMIENDA la inclusión de certificados de toda la cadena de certificación hasta un anclaje de veracidad.
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	F	
signerInfos SET OF	O	Al menos un signerInfo
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	F	(Valor no protegido)
digestAlgorithm DigestAlgorithmIdentifier,	O	**Algoritmos:** remitirse a la legislación nacional aplicable y, a efectos de directrices, a ETSI TS 102 176 y al informe ECRYPT2 D.SPA.7 para más recomendaciones.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	O	
attrType OBJECT IDENTIFIER,	O/F	**OBLIGATORIO**: id-contentType (con datos de identificación) id-messageDigest id-aa-ets-signingCertificateV2 o id-aa-signingCertificate OBLIGATORIO: signingTime **FACULTATIVO**: id-aa-ets-sigPolicyId Otros atributos facultativos según se definen en ETSI TS 101 733.
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmos:** remitirse a la legislación nacional aplicable y, a efectos de directrices, a ETSI TS 102 176 y al informe ECRYPT2 D.SPA.7 para más recomendaciones.
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	F	

SEQUENCE {
attrType OBJECT IDENTIFIER,
attrValues SET OF
AttributeValue
} OPTIONAL
}
}
	F	

SECCIÓN 3 – PAdES-PART 3 (BES/EPES):

La firma DEBERÁ utilizar una extensión de firma PAdES-BES (o -EPES) según se especifica en las especificaciones ETSI TS 102 778 PAdES-Part3 ([1]) y ajustarse a las especificaciones adicionales siguientes:

NO DEBERÁ utilizarse MD5 (RFC 1321) como algoritmo de compendio. Se remite a los firmantes a la legislación nacional aplicable y, a efectos de directrices, a ETSI TS 102 176 ([2]) y al informe ECRYPT2 D.SPA.x ([3]) para más recomendaciones sobre algoritmos y parámetros utilizables en firmas electrónicas.

Los atributos firmados DEBERÁN incluir una referencia al certificado digital X.509 v3 (RFC 5035) del firmante y el campo *SignedData.certificates* DEBERÁ incluir su valor.

([1]) ETSI TS 102 778-3 v1.2.1: PDF Advanced Electronic Signatures (PAdES), PAdES Enhanced – PAdES-Basic Electronic Signatures and PAdES-Explicit Policy Electronic Signatures Profiles.

([2]) ETSI TS 102 176: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; Part 2: «Secure channel protocols and algorithms for signature creation devices».

([3]) La versión más reciente es D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), de fecha 30 de marzo de 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

El instante de la firma se indica mediante el valor de la entrada **M** del diccionario de firmas.

En caso de que las firmas utilizadas por los Estados miembros se basen en un certificado reconocido, los objetos PKI (cadenas de certificados, datos de revocación, sellos temporales) incluidos en las firmas se pueden verificar utilizando la Lista de Confianza, de conformidad con la Decisión 2009/767/CE, del Estado miembro que supervisa o acredita al PSC que ha expedido el certificado del signatario.