DECISIONS

COMMISSION DECISION

of 25 February 2011

establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market

(notified under document C(2011) 1081)

(Text with EEA relevance)

(2011/130/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [1], and in particular Article 8(3) thereof,

Whereas:

(1) Service providers whose services fall within the scope of Directive 2006/123/EC must be able to complete, through the Points of Single Contact and by electronic means, the procedures and formalities necessary for the access to and the exercise of their activities. Within the limits established in Article 5(3) of Directive 2006/123/EC, there may still be cases where service providers have to submit original documents, certified copies or certified translations when completing such procedures and formalities. In those cases, service providers may need to submit documents signed electronically by competent authorities.

(2) The cross-border use of advanced electronic signatures supported by a qualified certificate is facilitated through Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market [2] which, inter alia, imposes an obligation on Member States to carry out risk assessments before requiring these electronic signatures from service providers and establishes rules for the acceptance by Member States of advanced electronic signatures based on qualified certificates, created with or without a secure signature creation device. However, Decision 2009/767/EC does not deal with formats of electronic signatures in documents issued by competent authorities, that need to be submitted by service providers when completing the relevant procedures and formalities.

(3) As competent authorities in Member States currently use different formats of advanced electronic signatures to sign their documents electronically, the receiving Member States that have to process these documents may face technical difficulties due to the variety of signature formats used. In order to allow service providers to complete their procedures and formalities across borders by electronic means, it is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically by competent authorities from other Member States. Defining a number of advanced electronic signature formats that need to be supported technically by the receiving Member State would allow greater automation and improve the cross-border interoperability of electronic procedures.

(4) Member States whose competent authorities use other electronic signature formats than those commonly supported, may have implemented validation means that allow their signatures to be verified also across borders. When this is the case and in order for the receiving Member States to be able to rely on these validation tools, it is necessary to make information on these tools available in an easily accessible way unless the necessary information is included directly in the electronic documents, in the electronic signatures or in the electronic document carriers.

(5) This Decision does not affect the determination by the Member States of what constitutes an original, a certified copy or a certified translation. Its objective is limited to facilitating the verification of electronic signatures if they are used in the originals, certified copies or certified translations that service providers may need to submit via the Points of Single Contact.

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

(6) For the purpose of allowing Member States to implement the necessary technical tools, it is appropriate that this Decision applies as of 1 August 2011.

(7) The measures provided for in this Decision are in accordance with the opinion of the Services Directive Committee,

HAS ADOPTED THIS DECISION:

Article 1

Reference format for electronic signatures

1. Member States shall put in place the necessary technical means allowing them to process electronically signed documents that service providers submit in the context of completing procedures and formalities through the Points of Single Contact as foreseen by Article 8 of Directive 2006/123/EC, and which are signed by competent authorities of other Member States with an XML or a CMS or a PDF advanced electronic signature in the BES or EPES format, that complies with the technical specifications set out in the Annex.

2. Member States whose competent authorities sign the documents referred to in paragraph 1 using other formats of electronic signatures than those referred to in that same paragraph, shall notify to the Commission existing validation possibilities that allow other Member States to validate the received electronic signatures online, free of charge and in a way that is understandable for non-native speakers unless the required information is already included in the document, in the electronic signature or in the electronic document carrier. The Commission will make that information available to all Member States.

Article 2

Application

This Decision shall apply from 1 August 2011.

Article 3

Addressees

This Decision is addressed to the Member States.

Done at Brussels, 25 February 2011.

For the Commission

Michel BARNIER

Member of the Commission

ANNEX

Specifications for an XML, CMS or PDF advanced electronic signature to be technically supported by the receiving Member State

Within the following part of the document the key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' are to be interpreted as described in RFC 2119 ([1]).

SECTION 1 — XAdES-BES/EPES

The signature is conform with the W3C XML Signature specifications ([2])

The signature MUST at least be a XAdES-BES (or -EPES) signature form as specified in the ETSI TS 101 903 XAdES specifications ([3]) and complies with all the following additional specifications:

The ds:CanonicalizationMethod that specifies the canonicalization algorithm applied to the SignedInfo element prior to performing signature calculations identifies one of the following algorithms only:

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#

Other algorithms or of 'With comments' versions of the above listed algorithms SHOULD NOT be used for the signature creation but SHOULD be supported for residual interoperability for the signature verification.

MD5 (RFC 1321) MUST NOT be used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines to ETSI TS 102 176 ([4]) and to the ECRYPT2 D.SPA.x report ([5]) for further recommendations on algorithms and parameters eligible for electronic signatures.

The use of *transforms* is restricted to the ones listed below:

Canonicalization transforms: see related specifications above;

Base64 encoding (http://www.w3.org/2000/09/xmldsig#base64);

Filtering:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): for compatibility reasons and conformance with XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): as a successor for XPath due to performance issues

Enveloped signature transform: (http://www.w3.org/2000/09/xmldsig#enveloped-signature).

XSLT (style sheet) **transform**.

The ds:KeyInfo element MUST include the signer's X.509 v3 digital certificate (i.e. its value and not only a reference to it).

The 'SigningCertificate' signed signature property MUST contain the digest value (CertDigest) and IssuerSerial of the signer's certificate stored in ds:KeyInfo and the optional URI in 'SigningCertificate' field MUST NOT be used.

The SigningTime signed signature property is present and contains the UTC expressed as xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

The DataObjectFormat element MUST BE present and contain MimeType sub-element.

In case the signatures used by Member States are based on a qualified certificate, the PKI objects (certificate chains, revocation data, time-stamps) that are included in the signatures are verifiable using the Trusted List, in accordance with Commission Decision 2009/767/EC, of the Member State who is supervising or accrediting the CSP having issued the signatory's certificate.

Table 1 summarises the specifications that a XAdES-BES/EPES signature must comply with to be supported technically by the receiving Member State.

([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]) Latest version is D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009 to 2010), dated 30 March 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Table 1

XAdES - BES (EPES)		**Common Minimum Requirements**
(ETSI TS 103 903 applies with the following profiled elements)		
M=Mandatory; O=Optional; R=Recommended; N=Not used		
ds: Signature ID	M	
ds: SignedInfo	M	
ds: CanonicalizationMethod	M	*All the following algorithms MUST be supported for signature verification, creation SHOULD restrict to one of these:* *- 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* *Other methods or "#WithComments" versions of the above methods SHOULD NOT be used.*
ds: SignatureMethod	M	***Algorithms:*** *refer to applicable national laws and for guidelines purposes to ETSI TS 102 176 and to ECRYPT2 D.SPA.7 report for further recommendations.*
ds: Reference URI	M	One reference to every original data object to be signed (URIs can point to external object as well), + reference to SignedProperties element
ds: Transforms	O	*Verifying applications MUST support all following transforms while signature creation application SHOULD restrict the use of those transforms to the following ones:* *- Canonicalization transforms: see above* *- Base64 encoding* *- XPath and XPath Filter 2.0* *- Enveloped signature transform* *- XSLT transforms*
ds: DigestMethod	M	***Algorithms:*** *refer to applicable national laws and for guidelines purposes to ETSI TS 102 176 and to ECRYPT2 D.SPA.7 report for further recommendations.*
ds: DigestValue	M	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	M	
ds: KeyInfo	M	MUST contain X509 certificate (SigningCertificate signed property MUST contain the digest value of this signer's certificate) Signer's certificate certification chain are RECOMMENDED to be provided as a hint for facilitating the validation process (X.509 certificates MUST be provided in this case).
ds: Object		
QualifyingProperties	M	
SignedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC (xsd: dateTime).
SigningCertificate	M	MUST contain the digest value of the signer's certificate stored in ds:KeyInfo and optional URI is omitted (Applications MAY look for/find the signer certificate in ds:KeyInfo on the basis of hash equivalence).
SignaturePolicyIdentifier	O	only for EPES form (and for upper forms built from EPES form)
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	M	When this field is used, applications SHALL ensure that data objects are shown to the user accordingly. When used, a MimeType child-element MUST be used.
CommitmentTypeIndication	O	
AllDataObjectsTimeStamp	O	
IndividualDataObjectTimeStamp	O	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	O	
UnsignedSignatureProperties		
CounterSignature	O	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Signature topology - Packaging signed original files and signatures		
SignatureEnveloped		All MUST be supported
SignatureEnveloping		
SignatureDetached		

SECTION 2 — CAdES-BES/EPES

The signature is conform with the Cryptographic Message Syntax (CMS) Signature specifications [1].

The signature uses CAdES-BES (or -EPES) signature attributes as specified in the ETSI TS 101 733 CAdES specifications [2] and complies with the additional specifications as indicated in Table 2 below.

All attributes of CAdES which are included in the archive timestamp hash calculation (ETSI TS 101 733 V1.8.1 Annex K) MUST be in DER encoding and any other can be in BER to simplify one-pass processing of CAdES.

MD5 (RFC 1321) MUST NOT be used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines to ETSI TS 102 176 [3] and to the ECRYPT2 D.SPA.x report [4] for further recommendations on algorithms and parameters eligible for electronic signatures.

The signed attributes MUST include a reference to the signer's X.509 v3 digital certificate (RFC 5035) and *SignedData.certificates* field MUST include its value.

The SigningTime signed attribute MUST be present and MUST contain the UTC expressed as in http://tools.ietf.org/html/rfc5652#section-11.3.

The ContentType signed attribute MUST be present and contains id-data (http://tools.ietf.org/html/rfc5652#section-4) where the data content type is intended to refer to arbitrary octet strings, such as UTF-8 text or ZIP container with MimeType sub-element.

In case the signatures used by Member States are based on a qualified certificate, the PKI objects (certificate chains, revocation data, time-stamps) that are included in the signatures are verifiable using the Trusted List, in accordance with Commission Decision 2009/767/EC, of the Member State who is supervising or accrediting the CSP having issued the signatory's certificate.

---

[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] Latest version is D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009 to 2010), dated 30 March 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Table 2

CAdES - BES (EPES)		**Common Minimum Requirements**
(ETSI TS 101 733 applies with the following profiled elements)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
M=Mandatory; O=Optional; R=Recommended; N=Not used		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	M	**Algorithms**: refer to applicable national laws and for guidelines purposes to ETSI TS 102 176 and to ECRYPT2 D.SPA.7 report for further recommendations.
encapContentInfo SEQUENCE {		
eContentType ContentType,	M	id-Data
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	M/N	The ContentType signed attribute is present and contains id-data (http://tools.ietf.org/html/rfc5652#section-4) where the data content type is intended to refer to arbitrary octet strings, such as UTF-8 text or ZIP container with MimeType sub-element
-- External Data (if signature detached)*		if detached signature otherwise not present. * External data means data protected by a detached signature that is not included in the CAdES signature eContent. It is recommended to include signed external data together with the signature in ZIP file.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	M	MUST contain X509 certificate from the signer. Inclusion of Certificates from the entire certification chain up to a trust anchor is RECOMMENDED.
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	O	
signerInfos SET OF	M	At least one signerInfo
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	O	(Not protected value)
digestAlgorithm DigestAlgorithmIdentifier,	M	**Algorithms**: refer to applicable national laws and for guidelines purposes to ETSI TS 102 176 and to ECRYPT2 D.SPA.7 report for further recommendations.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	M	
attrType OBJECT IDENTIFIER,	M/O	**MUST**: id-contentType (with id data) id-messageDigest id-aa-ets-signingCertificateV2 or id-aa-signingCertificate MUST: signingTime **OPTIONAL**: id-aa-ets-sigPolicyId Other optional attributes as defined in ETSI TS 101 733.
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algorithms**: refer to applicable national laws and for guidelines purposes to ETSI TS 102 176 and to ECRYPT2 D.SPA.7 report for further recommendations.
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	O	
SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }	O	

SECTION 3 — PAdES-PART 3 (BES/EPES)

The signature MUST use a PAdES-BES (or -EPES) signature extension as specified in the ETSI TS 102 778 PAdES-Part3 specifications ([1]) and complies with the following additional specifications:

MD5 (RFC 1321) MUST NOT be used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines, to ETSI TS 102 176 ([2]) and to the ECRYPT2 D.SPA.x report ([3]) for further recommendations on algorithms and parameters eligible for electronic signatures.

The signed attributes MUST include a reference to the signer's X.509 v3 digital certificate (RFC 5035) and *SignedData.certificates* field MUST include its value.

([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]) Latest version is D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009 to 2010), dated 30 March 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

The time of signing is indicated by the value of the **M** entry in the signature dictionary.

In case the signatures used by Member States are based on a qualified certificate, the PKI objects (certificate chains, revocation data, time-stamps) that are included in the signatures are verifiable using the Trusted List, in accordance with Decision 2009/767/EC, of the Member State who is supervising or accrediting the CSP having issued the signatory's certificate.