Draft

COMMISSION DECISION

of […]

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

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. When completing such procedures and formalities, service providers may be required to submit original documents, certified copies or certified translations, within the limits established in Article 5. 3 of Directive 2006/123/EC. In this context, service providers may need to submit electronically signed documents which in many cases are issued by public authorities.

(2) The cross-border use of advanced electronic signatures supported by a qualified certificate is facilitated through Decision 2009/767/EC[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. The Decision does not deal with the issue of advanced electronic signature formats.

1 OJ L 376, 27.12.2006, p. 36.

2 Decision 2009/767/EC 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 , OJ L 299, 14.11.2009, p. 18.

(3) As public administrations in Member States currently use different formats of advanced electronic signatures to sign electronically their documents, 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 electronically their procedures and formalities across borders, 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 public administrations from other Member States. Defining a number of advanced electronic signature formats that need to be supported technically at the receiving side would allow greater automation and improve the cross-border interoperability of electronic procedures.

(4) Member States whose public authorities use other electronic signature formats than those commonly supported, may have implemented validation means that allow their signatures to be verified also across border. In order for the receiving Member States to be able to rely on the validation tools in other Member States, it is necessary to make information available on these tools in an easily accessible way. Member States may also facilitate the validation of their signatures by including the necessary information directly in the documents or their signatures.

(5) 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, as a minimum, 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 public 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 public administrations 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 validation possibilities that allow other Member States to validate the received electronic signatures online, for free and in a way that is understandable for non-native speakers, unless the required information is already included in the document or in the electronic signature. The Commission will make that information available to all Member States.

Article 2

Application

This Decision shall apply from …..

Article 3

Addressees

This Decision is addressed to the Member States.

Done at Brussels, […]

For the Commission
[…]
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[3].

Section 1 – XAdES-BES/EPES:

- The signature is conform with the W3C XML Signature specifications[4]
- The signature uses a XAdES-BES (or -EPES) signature extension as specified in the ETSI TS 101 903 XAdES specifications[5] and complies with all the following additional specifications:
    - Unique identifiers are used for the different XML elements that require an identifier attribute, e.g. to allow for multiple signatures to co-exist within the same XML document;
    - 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) is not used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines to ETSI TS 102

[3] IETF RFC 2119: "Key words for use in RFCs to indicate Requirements Levels".
4 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/.

5 ETSI TS 101 903 v1.4.1: XML Advanced Electronic Signatures (XAdES).

176[6] and to the ECRYPT2 D.SPA.7 report[7] for further recommendations on algorithms and parameters eligible for electronic signatures.

- There should be one ds:Reference element for each original data object to be signed (URIs can point to an external object as well), including a reference to the SignedProperties element.
- 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-xpath19991116): 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 includes the signer's X.509 v3 digital certificate (i.e. its value and not only a reference to it);
- The "SigningCertificate" signed signature property contains the digest value (CertDigest) and IssuerSerial of the signer's certificate stored in ds:KeyInfo and the optional URI in "SigningCertificate" field is omitted;
- The SigningTime signed signature property is present and contains the UTC expressed as Zulu time zone time (xsd:dateTime);
- The DataObjectFormat element is present as critical and contains MimeType sub-element;

- The PKI objects (certificate chains, revocation data, time-stamps) that are included in the signatures of Member States are verifiable using the Trusted List[8] ,in accordance with Decision 2009/767/EC, of the Member State who is supervising or accrediting the CSP having issued the signatory's certificate.

---

6 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".

7 D.SPA.7 ECRYPT2 Yearly Report on Algorithms and Key sizes (2008-2009), dated 31 July 2009 (http://www.ecrypt.eu.org/documents/D.SPA.7.pdf).

8 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. OJ L 299 of 14.11.2009, p. 18.

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

XAdES - BES (EPES)		Common Minimum Requirements
(ETSI TS 103 903 applies with the following profiled elements)		
M=Mandatory; O=Optional; C=Critical (for Verifiers);R=Recommended; N=Not used		
ds: Signature ID	M	With Id parameter. Unique identifiers SHOULD be used.
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	***Digest algorithms & Signature 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-C	*MUST be treated when present. 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	***Digest 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	Base64 encoded
/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	*embedded bag or reference*
SignedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC expressed as Zulu (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-C	When this field is used, applications SHALL ensure that data objects are shown to the user accordingly. When used, MimeType sub-elements 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		

Table 1

Section 2 – CAdES-BES/EPES:

- The signature is conform with the Cryptographic Message Syntax (CMS) Signature specifications[9]

- The signature uses CAdES-BES (or -EPES) signature attributes as specified in the ETSI TS 101 733 CAdES specifications[10] and complies with the additional specifications as indicated in Table 2 below.

- The encoding of ASN.1 data elements MUST be in DER not only for data which are included in hash computations but also for all data which are defined in CMS structure.

- MD5 (RFC 1321) is not used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines to ETSI TS 102 176[11] and to the ECRYPT2 D.SPA.7 report[12] for further recommendations on algorithms and parameters eligible for electronic signatures.

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

- The SigningTime signed attribute is present and contains the UTC expressed as Zulu time zone time (http://tools.ietf.org/html/rfc5652#section-11.3);

- 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;

- The PKI objects (certificate chains, revocation data, time-stamps) that are included in the signatures of Member States are verifiable using the Trusted List[13] ,in accordance with Decision 2009/767/EC, of the Member State who is supervising or accrediting the CSP having issued the signatory's certificate.

9 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.

10 ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES).

11 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".

12 D.SPA.7 ECRYPT2 Yearly Report on Algorithms and Key sizes (2008-2009), dated 31 July 2009 (http://www.ecrypt.eu.org/documents/D.SPA.7.pdf).

13 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. OJ L 299 of 14.11.2009, p. 18.

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; C=Critical (for Verifiers);R=Recommended; N=Not used		
`SignedData ::= SEQUENCE {`		
`version CMSVersion,`		
`digestAlgorithms DigestAlgorithmIdentifiers,`	M	**Digest 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 CertificateRevocationLists OPTIONAL,`	O	
`signerInfos SET OF`	M	At least one signerInfo
`SEQUENCE { -- SignerInfo`		
`version CMSVersion,`		
`sid SignerIdentifier,`	O	(Not protected value)
`digestAlgorithm DigestAlgorithmIdentifier,`	M	**Digest 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	DER encoded
`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,`		DER encoded
`signatureAlgorithm SignatureAlgorithmIdentifier,`		**Digest 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	

Table 2

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[14]and complies with the following additional specifications:

    - MD5 (RFC 1321) is not used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines, to ETSI TS 102 176[15] and to the ECRYPT2 D.SPA.7 report[16] for further recommendations on algorithms and parameters eligible for electronic signatures.

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

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

- The PKI objects (certificate chains, revocation data, time-stamps) that are included in the signatures of Member States are verifiable using the Trusted List[17] ,in accordance with Decision 2009/767/EC, of the Member State who is supervising or accrediting the CSP having issued the signatory's certificate.

14 ETSI TS 102 778: PDF Advanced Electronic Signatures (PAdES), PAdES Enhanced – PAdES-Basic Electronic Signatures and PAdES-Explicit Policy Electronic Signatures Profiles.

15 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".

16 D.SPA.7 ECRYPT2 Yearly Report on Algorithms and Key sizes (2008-2009), dated 31 July 2009 (http://www.ecrypt.eu.org/documents/D.SPA.7.pdf).

17 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. OJ L 299 of 14.11.2009, p. 18.