DÉCISIONS

DÉCISION DE LA COMMISSION

du 25 février 2011

établissant des exigences minimales pour le traitement transfrontalier des documents signés électroniquement par les autorités compétentes conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur

[notifiée sous le numéro C(2011) 1081]

(Texte présentant de l'intérêt pour l'EEE)

(2011/130/UE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu la directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur [1], et notamment son article 8, paragraphe 3,

considérant ce qui suit:

(1) Les prestataires de services dont les services relèvent de la directive 2006/123/CE doivent pouvoir effectuer, via les guichets uniques et par voie électronique, les procédures et les formalités nécessaires à l'accès à leurs activités et à l'exercice de ces activités. Dans les limites fixées par l'article 5, paragraphe 3, de la directive 2006/123/CE, il peut subsister des cas où les prestataires de services doivent présenter des documents originaux, des copies certifiées conformes ou des traductions certifiées conformes lorsqu'ils effectuent ces procédures et formalités. Dans de tels cas, les prestataires de services peuvent être tenus de présenter des documents signés électroniquement par des autorités compétentes.

(2) L'utilisation transfrontalière de signatures électroniques avancées associées à un certificat qualifié est facilitée par la décision 2009/767/CE de la Commission du 16 octobre 2009 établissant des mesures destinées à faciliter l'exécution de procédures par voie électronique par l'intermédiaire des «guichets uniques» conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur [2], laquelle impose notamment aux États membres d'effectuer une évaluation des risques avant d'exiger des prestataires de services qu'ils utilisent ces signatures électroniques, et établit des règles d'acceptation, par les États membres, de signatures électroniques avancées basées sur des certificats qualifiés et créées avec ou sans dispositif sécurisé de création de signature. Toutefois, la décision 2009/767/CE ne traite pas des formats des signatures électroniques des documents, émis par les autorités compétentes, que doivent présenter les prestataires de services lorsqu'ils effectuent les procédures et formalités requises.

(3) Les autorités compétentes des États membres utilisant actuellement différents formats de signatures électroniques avancées pour signer électroniquement leurs documents, les États membres destinataires qui doivent traiter ces documents peuvent être confrontés à des difficultés techniques en raison de la variété de formats de signature utilisés. Afin de permettre aux prestataires de services d'effectuer par voie électronique les procédures et les formalités transfrontalières requises, il faut veiller à ce qu'au moins certains formats de signatures électroniques avancées puissent être traités techniquement par les États membres lorsqu'ils reçoivent des documents signés électroniquement par les autorités compétentes d'autres États membres. En spécifiant un certain nombre de formats de signature électronique avancée que les États membres destinataires seraient tenus de pouvoir exploiter techniquement, on favoriserait l'automatisation et on améliorerait l'interopérabilité transfrontalière des procédures électroniques.

(4) Les États membres dont les autorités compétentes utilisent des formats de signature électronique autres que ceux couramment employés peuvent avoir mis en place des moyens de validation permettant de vérifier leurs signatures, y compris de manière transfrontalière. Dans ce cas, et afin que les États membres destinataires puissent recourir à ces outils de validation, les informations sur ces outils doivent être rendues aisément accessibles, sauf si elles sont incluses directement dans les documents électroniques, dans les signatures électroniques ou dans les supports électroniques des documents.

(5) La présente décision n'affecte en rien la détermination, par les États membres, de ce qui constitue un original, une copie certifiée conforme ou une traduction certifiée conforme. Son objet se borne à faciliter la vérification de signatures électroniques lorsque celles-ci sont utilisées dans des originaux, des copies certifiées conformes ou des traductions certifiées conformes que les prestataires de services peuvent être tenus de présenter via les guichets uniques.

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

(6) Afin de permettre aux États membres de mettre en œuvre les outils techniques requis, il convient que la présente décision s'applique à compter du 1er août 2011.

(7) Les mesures prévues par la présente décision sont conformes à l'avis du comité «directive services»,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Format de référence des signatures électroniques

1. Les États membres mettent en place les moyens techniques leur permettant de traiter les documents qui leur sont soumis par des prestataires de services dans le cadre des procédures et des formalités qu'ils effectuent via les guichets uniques conformément à l'article 8 de la directive 2006/123/CE et qui sont signés électroniquement par les autorités compétentes d'autres États membres au moyen d'une signature électronique avancée XML, CMS ou PDF au format BES ou EPES conforme aux spécifications techniques figurant en annexe.

2. Les États membres dont les autorités compétentes signent les documents visés au premier alinéa en utilisant d'autres formats de signature électronique que ceux visés audit alinéa notifient à la Commission les possibilités de validation existantes permettant aux autres États membres de valider en ligne, gratuitement et sans que la connaissance de la langue native soit nécessaire, les signatures électroniques reçues, sauf si les informations requises sont incluses dans le document, dans la signature électronique ou dans le support électronique du document. La Commission met ces informations à la disposition de tous les États membres.

Article 2

Application

La présente décision s'applique à compter du 1er août 2011.

Article 3

Destinataires

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 25 février 2011.

Par la Commission

Michel BARNIER

Membre de la Commission

ANNEXE

Spécifications à respecter par les signatures électroniques avancées XML, CMS ou PDF devant être techniquement exploitables par les États membres destinataires

Dans la présente annexe, le mot-clé «DOIT» et ses différentes formes grammaticales sont à comprendre dans le sens des termes «MUST», «REQUIRED» et «SHALL» tels que décrits dans le RFC 2119; le mot-clé «NE DOIT PAS» et ses différentes formes grammaticales sont à comprendre dans le sens des termes «MUST NOT» et «SHALL NOT» tels que décrits dans le RFC 2119; les mots-clés «DEVRAIT» et «RECOMMANDÉ» et leurs différentes formes grammaticales sont à comprendre dans le sens des termes «SHOULD» et «RECOMMENDED» tels que décrits dans le RFC 2119; le mot-clé «NE DEVRAIT PAS» et ses différentes formes grammaticales sont à comprendre dans le sens des termes «SHOULD NOT» et «NOT RECOMMENDED» tels que décrits dans le RFC 2119 ([1]).

SECTION 1 — XAdES-BES/EPES

La signature est conforme aux spécifications des signatures XML du W3C ([2]).

La signature DOIT au moins être une signature de forme XAdES-BES (ou –EPES) telle que définie dans les spécifications XAdES ETSI TS 101 903 ([3]) et respecter toutes les spécifications supplémentaires suivantes:

La méthode ds:CanonicalizationMethod qui spécifie l'algorithme de mise en forme canonique appliqué à l'élément SignedInfo avant le calcul de la signature désigne un des algorithmes suivants:

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#

Les autres algorithmes et les versions «with comments» des algorithmes ci-dessus NE DEVRAIENT PAS être utilisés pour la création de la signature mais DEVRAIENT être pris en charge aux fins de l'interopérabilité résiduelle de la vérification de la signature.

MD5 (RFC 1321) NE DOIT PAS être utilisé en tant qu'algorithme de hachage. Les signataires sont invités à se référer à la réglementation nationale applicable et à ETSI TS 102 176 ([4]) et au rapport ECRYPT2 D.SPA.x ([5]) pour d'autres recommandations sur les algorithmes et paramètres susceptibles d'être utilisés dans le contexte des signatures électroniques.

L'utilisation des transformations *(transforms)* est limitée à celles énumérées ci-après:

Transformations de mise en forme canonique: voir les spécifications afférentes ci-dessus;

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

Filtrage:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): pour des raisons de compatibilité et de conformité avec XMLDSig;

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): en tant que successeur de XPath pour des questions de performance.

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

XSLT transform.

L'élément ds:KeyInfo DOIT inclure le certificat numérique X.509 v3 du signataire (autrement dit sa valeur, et pas seulement une référence au certificat).

La propriété signée «SigningCertificate» de la signature DOIT comprendre la valeur hachée (CertDigest) et l'IssuerSerial du certificat du signataire stocké dans ds:KeyInfo. Le champ optionnel URI de «SigningCertificate» NE DOIT PAS être utilisé.

La propriété signée «SigningTime» de la signature est présente et contient le temps UTC exprimé en tant que xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

L'élément DataObjectFormat DOIT être présent et contenir le sous-élément MimeType.

Au cas où les signatures utilisées par les États membres sont basées sur un certificat qualifié, les objets PKI (chaînes de certificats, données de révocation, horodatages) inclus dans les signatures sont vérifiables, conformément à la décision 2009/767/CE, au moyen de la liste de confiance de l'État membre qui contrôle ou accrédite le CSP qui a émis le certificat du signataire.

Le tableau 1 résume les spécifications qu'une signature XAdES-BES/EPES doit respecter afin de pouvoir être exploitée techniquement par l'État membre de destination.

([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; Partie 1: «Hash functions and asymmetric algorithms»; Partie 2: «Secure channel protocols and algorithms for signature creation devices».
([5]) La dernière version du 30 mars 2010 est «D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010)» (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tableau 1

XAdES - BES (EPES)		**Exigences communes minimales**
(ETSI TS 103 903 s'applique avec les éléments de profil suivants)		
E=Exigé; O=Optionnel; R=Recommandé; N=Non utilisé		
ds: Signature ID	E	
ds: SignedInfo	E	
ds: CanonicalizationMethod	E	*Tous les algorithmes suivants DOIVENT pouvoir être pris en charge pour la vérification des signatures, la création DEVRAIT être limitée à l'une des méthodes suivantes:* *—éxclusive 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* *Aucune autre méthode ni les versions "#WithComments" des méthodes ci-dessus NE DEVRAIENT être utilisées*
ds: SignatureMethod	E	***Algorithmes:*** *se référer aux réglementations nationales applicables et, en matière de lignes directrices, à ETSI TS 102 176 et au rapport ECRYPT2 D.SPA.7 pour d'autres recommandations.*
ds: Reference URI	E	Une référence à chaque objet de données original devant être signé (les URI peuvent également pointer vers des objets externes), plus une référence à l'élément SignedProperties
ds: Transforms	O	*Les applications de vérification DOIVENT prendre en charge toutes les transformations suivantes tandis que l'application de création des signatures DEVRAIT limiter l'utilisation de ces transformations aux suivantes:* *— transformations de mise en forme canonique: voir ci-dessus* *— codage Base64* *— XPath et XPath Filter 2.0* *— Enveloped signature transform* *—transformations XSLT*
ds: DigestMethod	E	***Algorithmes:*** *se référer aux réglementations nationales applicables et, en matière de lignes directrices, à ETSI TS 102 176 et au rapport ECRYPT2 D.SPA.7 pour d'autres recommandations.*
ds: DigestValue	E	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	E	
ds: KeyInfo	E	DOIT contenir un certificat X.509 (la propriété signée SigningCertificate DOIT contenir la valeur hachée du certificat de ce signataire) Il est RECOMMANDÉ de fournir la chaîne de certification du certificat du signataire afin de faciliter le processus de validation (les certificats X.509 DOIVENT être fournis dans ce cas).
ds: Object		
QualifyingProperties	E	
SignedProperties	E	E
SignedSignatureProperties	E	E
SigningTime	E	UTC (xsd: dateTime).
SigningCertificate	E	DOIT contenir la valeur hachée du certificat du signataire stockée dans ds:KeyInfo et l'URI facultative est omise (les applications PEUVENT chercher/trouver le certificat du signataire dans ds:KeyInfo sur la base de l'équivalence des hachages).
SignaturePolicyIdentifier	O	uniquement pour la forme EPES (et les formes supérieures construites sur la forme EPES)
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	E	Lorsque ce champ est utilisé, les applications DOIVENT faire en sorte que les objets de données soient montrés à l'utilisateur en conséquence. Lorsqu'il est utilisé, un élément fille MimeType DOIT être utilisé.
CommitmentTypeIndication	O	
AllDataObjectsTimeStamp	O	
IndividualDataObjectTimeStamp	O	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	O	
UnsignedSignatureProperties		
CounterSignature	O	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Topologie de signature – packaging des fichiers originaux et des signatures signés		
SignatureEnveloped		DOIVENT tous être pris en charge
SignatureEnveloping		
SignatureDetached		

SECTION 2 — CAdES-BES/EPES

La signature est conforme aux spécifications de la syntaxe CMS (Cryptographic Message Syntax) ([1]).

La signature utilise les attributs de signature CAdES-BES (ou -EPES) tels que définis dans les spécifications CAdES ETSI TS 101 733 ([2]) et respecte les spécifications supplémentaires indiquées dans le tableau 2 ci-dessous.

Tous les attributs CAdES qui sont inclus dans le calcul du hachage de l'horodatage de l'archive (ETSI TS 101 733 V1.8.1, annexe K) DOIVENT être codés en DER; les autres peuvent être codés en BER pour simplifier le traitement CAdES en un seul passage.

MD5 (RFC 1321) NE DOIT PAS être utilisé en tant qu'algorithme de hachage. Les signataires sont invités à se référer à la réglementation nationale applicable et, en matière de lignes directrices, à ETSI TS 102 176 ([3]) et au rapport ECRYPT2 D.SPA.x ([4]) pour d'autres recommandations sur les algorithmes et paramètres susceptibles d'être utilisés dans le contexte des signatures électroniques.

Les attributs signés DOIVENT inclure une référence au certificat numérique X.509 v3 (RFC 5035) du signataire et le champ *SignedData.certificates* DOIT inclure sa valeur.

L'attribut signé SigningTime DOIT être présent et DOIT contenir le temps UTC exprimé conformément à http://tools.ietf.org/html/rfc5652#section-11.3.

L'attribut signé ContentType DOIT être présent et contenir id-data (http://tools.ietf.org/html/rfc5652#section-4), le type de contenu de données servant à se référer à des chaînes d'octets arbitraires, par exemple un texte UTF-8 ou un conteneur Zip avec un sous-élément MimeType.

Au cas où les signatures utilisées par les États membres sont basées sur un certificat qualifié, les objets PKI (chaînes de certificats, données de révocation, horodatages) inclus dans les signatures sont vérifiables, conformément à la décision 2009/767/CE, au moyen de la liste de confiance de l'État membre qui contrôle ou accrédite le CSP qui a émis le certificat du signataire.

([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; Partie 1: «Hash functions and asymmetric algorithms»; Partie 2: «Secure channel protocols and algorithms for signature creation devices».

([4]) La dernière version du 30 mars 2010 est «D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010)» (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tableau 2

CAdES - BES (EPES)		Exigences communes minimales
(ETSI TS 101 733 s'applique avec les éléments de profil suivants)		
ASN.1		
`ContentInfo ::= SEQUENCE {`		
`contentType ContentType, -- id-signedData`		
`content [0] EXPLICIT ANY DEFINED BY contentType }`		
E=Exigé; O=Optionnel; R=Recommandé; N=Non utilisé		
`SignedData ::= SEQUENCE {`		
`version CMSVersion,`		
`digestAlgorithms DigestAlgorithmIdentifiers,`	E	**Algorithmes**: se référer aux réglementations nationales applicables et, en matière de lignes directrices, à ETSI TS 102 176 et au rapport ECRYPT2 D.SPA.7 pour d'autres recommandations.
`encapContentInfo SEQUENCE {`		
`eContentType ContentType,`	E	id-Data
`eContent [0] EXPLICIT OCTET STRING OPTIONAL -- non présent si la signature est détachée },`	E/N	L'attribut signé ContentType DOIT être présent et contenir id-data (http://tools.ietf.org/html/rfc5652#section-4), le type de contenu de données sert à se référer à des chaînes d'octets arbitraires, par exemple un texte UTF-8 ou un conteneur Zip avec un sous-élément MimeType.
`-- Données externes (en cas de signature détachée)*`		En cas de signature détachée; sinon, non présent. * Données externes: données protégées par une signature détachée non incluse dans le contenu électronique de signature CAdES. Il est recommandé d'inclure les données externes signées en même temps que la signature dans un fichier ZIP.
`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	E	DOIT contenir le certficat X.509 du signataire. Il est RECOMMANDÉ d'inclure les certificats de toute la chaîne de certificats jusqu'à une ancre de confiance.
`crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,`	O	
`signerInfos SET OF`	E	Au moins un signerInfo
`SEQUENCE { -- SignerInfo`		
`version CMSVersion,`		
`sid SignerIdentifier,`	O	(Valeur non protégée)
`digestAlgorithm DigestAlgorithmIdentifier,`	E	**Algorithmes**: se référer aux réglementations nationales applicables et, en matière de lignes directrices, à ETSI TS 102 176 et au rapport ECRYPT2 D.SPA.7 pour d'autres recommandations.
`signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF`		
`SEQUENCE { -- Attribute`	E	
`attrType OBJECT IDENTIFIER,`	E/O	**EXIGÉ**: id-contentType (avec id data) id-messageDigest id-aa-ets-signingCertificateV2 ou id-aa-signingCertificate EXIGÉ: signingTime **OPTIONNEL**: id-aa-ets-sigPolicyId Autres attributs optionnels tels que définis dans ETSI TS 101 733.
`attrValues SET OF AttributeValue } OPTIONAL,`		
`signatureAlgorithm SignatureAlgorithmIdentifier,`		**Algorithmes**: se référer aux réglementations nationales applicables et, en matière de lignes directrices, à ETSI TS 102 176 et au rapport ECRYPT2 D.SPA.7 pour d'autres recommandations.
`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)

La signature DOIT utiliser une extension de signature PAdES-BES (ou -EPES) telle que définie dans les spécifications PAdES-Part3 ETSI TS 102 778 ([1]) et respecter toutes les spécifications supplémentaires suivantes:

MD5 (RFC 1321) NE DOIT PAS être utilisé en tant qu'algorithme de hachage. Les signataires sont invités à se référer à la réglementation nationale applicable et, en matière de lignes directrices, à ETSI TS 102 176 ([2]) et au rapport ECRYPT2 D.SPA.x ([3]) pour d'autres recommandations sur les algorithmes et paramètres susceptibles d'être utilisés dans le contexte des signatures électroniques.

Les attributs signés DOIVENT inclure une référence au certificat numérique X.509 v3 (RFC 5035) du signataire et le champ *SignedData.certificates* DOIT inclure sa valeur.

([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; Partie 1: «Hash functions and asymmetric algorithms»; Partie 2: «Secure channel protocols and algorithms for signature creation devices».

([3]) La dernière version du 30 mars 2010 est «D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010)» (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Le moment de la signature est indiqué par la valeur de l'entrée **M** dans le dictionnaire de signature.

Au cas où les signatures utilisées par les États membres sont basées sur un certificat qualifié, les objets PKI (chaînes de certificats, données de révocation, horodatages) inclus dans les signatures sont vérifiables, conformément à la décision 2009/767/CE, au moyen de la liste de confiance de l'État membre qui contrôle ou accrédite le CSP qui a émis le certificat du signataire.