DECISÕES

DECISÃO DA COMISSÃO

de 25 de Fevereiro de 2011

que estabelece requisitos mínimos para o processamento transfronteiras de documentos assinados electronicamente pelas autoridades competentes nos termos da Directiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno

[notificada com o número C(2011) 1081]

(Texto relevante para efeitos do EEE)

(2011/130/UE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta a Directiva 2006/123/CE do Parlamento Europeu e do Conselho, de 12 de Dezembro de 2006, relativa aos serviços no mercado interno [1], nomeadamente o seu artigo 8.º, n.º 3,

Considerando o seguinte:

(1) Os prestadores de serviços cujos serviços se encontram abrangidos pela Directiva 2006/123/CE devem poder cumprir os procedimentos e formalidades necessários ao acesso às suas actividades e ao seu exercício através de balcões únicos e electronicamente. Dentro dos limites previstos no artigo 5.º, n.º 3, da Directiva 2006/123/CE, poderá ainda haver situações em que os prestadores de serviços têm de entregar documentos originais, cópias autenticadas ou traduções autenticadas originais para cumprirem esses procedimentos e formalidades. Nestas circunstâncias, os prestadores de serviços poderão ter de entregar documentos assinados electronicamente pelas autoridades competentes.

(2) A utilização transfronteiras de assinaturas electrónicas avançadas baseadas num certificado qualificado é prevista na Decisão 2009/767/CE da Comissão, de 16 de Outubro de 2009, que determina medidas destinadas a facilitar a utilização de procedimentos informatizados através de «balcões únicos», nos termos da Directiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno [2] que, nomeadamente, impõe aos Estados-Membros a obrigatoriedade de realizarem uma avaliação dos riscos antes de exigirem aos prestadores de serviços tais assinaturas electrónicas e estabelece as regras de aceitação pelos Estados-Membros de assinaturas electrónicas avançadas baseadas num certificado qualificado, criadas com ou sem um dispositivo seguro de criação de assinaturas. No entanto, a Decisão 2009/767/CE não aborda a questão dos formatos das assinaturas electrónicas em documentos emitidos por autoridades competentes que têm de ser entregues pelos prestadores de serviços no cumprimento dos procedimentos e formalidades em questão.

(3) Como as autoridades competentes nos Estados-Membros utilizam actualmente diferentes formatos de assinaturas electrónicas avançadas para assinar electronicamente os seus documentos, os Estados-Membros que recebem e têm de processar estes documentos poderão enfrentar dificuldades técnicas decorrentes da variedade de formatos de assinaturas existentes. Para permitir aos prestadores de serviços cumprir transfronteiras os seus procedimentos e formalidades electronicamente, é necessário garantir que pelo menos um determinado número de formatos de assinaturas electrónicas avançadas são suportados tecnicamente pelos Estados-Membros quando recebem documentos assinados electronicamente pelas autoridades competentes de outros Estados-Membros. A definição de um certo número de formatos de assinaturas electrónicas avançadas que os Estados-Membros destinatários devem poder suportar tecnicamente contribuirá para uma maior automatização e uma melhor interoperabilidade transfronteiras dos procedimentos electrónicos.

(4) Os Estados-Membros cujas autoridades competentes utilizam assinaturas electrónicas em formatos diferentes dos formatos mais comuns poderão dispor de meios de validação estabelecidos que permitam que as suas assinaturas sejam verificadas também nos outros países. Sempre que for esse o caso e para que os Estados-Membros destinatários possam confiar nesses instrumentos de validação, é necessário disponibilizar informações sobre tais ferramentas de forma facilmente acessível, a não ser que a informação necessária esteja disponível directamente nos documentos electrónicos, nas assinaturas electrónicas ou nos suportes dos documentos electrónicos.

(5) A presente decisão não afecta a forma como os Estados-Membros determinam o que constitui um documento original, uma cópia autenticada ou uma tradução autenticada. Limita-se a tentar facilitar o processo de verificação das assinaturas electrónicas caso elas sejam utilizadas nos documentos originais, nas cópias autenticadas ou nas traduções autenticadas que os prestadores de serviços poderão ter de entregar através dos balcões únicos.

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

(6) Para permitir aos Estados-Membros estabelecerem as ferramentas técnicas necessárias, é conveniente que a presente decisão entre em vigor a partir de 1 de Agosto de 2011.

(7) As medidas previstas na presente decisão estão em conformidade com o parecer do Comité da Directiva Serviços.

ADOPTOU A PRESENTE DECISÃO:

Artigo 1.º

Formato de referência para as assinaturas electrónicas

1. Os Estados-Membros devem estabelecer os meios técnicos necessários que lhes permitam processar documentos assinados electronicamente entregues pelos prestadores de serviços no cumprimento de procedimentos e formalidades através de balcões únicos, nos termos do artigo 8.º da Directiva 2006/123/CE, e que sejam assinados pelas autoridades competentes de outros Estados-Membros com uma assinatura electrónica avançada XML ou CMS ou PDF no formato BES ou EPES que satisfaça as especificações técnicas descritas no anexo.

2. Os Estados-Membros cujas autoridades competentes assinam os documentos referidos no n.º 1 com assinaturas electrónicas em formatos diferentes dos referidos no mesmo número devem informar a Comissão acerca das formas de validação existentes que permitam aos restantes Estados-Membros validar gratuitamente, em linha e de forma compreensível para falantes não nativos, as assinaturas electrónicas recebidas, a não ser que a informação necessária já esteja incluída no documento, na assinatura electrónica ou no suporte do documento electrónico. A Comissão disponibilizará esta informação a todos os Estados-Membros.

Artigo 2.º

Aplicação

A presente decisão é aplicável a partir de 1 de Agosto de 2011.

Artigo 3.º

Destinatários

Os Estados-Membros são os destinatários da presente decisão.

Feito em Bruxelas, em 25 de Fevereiro de 2011.

Pela Comissão

Michel BARNIER

Membro da Comissão

ANEXO

Especificações que uma assinatura electrónica avançada em XML, CMS ou PDF deve cumprir para ser suportada tecnicamente pelo Estado-Membro destinatário

Na parte do documento que se segue as palavras-chave «DEVE», «NÃO DEVE», «OBRIGATÓRIO», «DEVERÁ», «NÃO DEVERÁ», «DEVERIA», «NÃO DEVERIA», «RECOMENDADO», «PODE» e «FACULTATIVO» devem ser interpretadas tal como descritas no RFC 2119 ([1]).

SECÇÃO 1 – XAdES-BES/EPES

A assinatura está em conformidade com as especificações de assinaturas XML do W3C ([2])

A assinatura DEVE pelo menos estar no formato de assinatura XAdES-BES (ou -EPES), de acordo com a especificação técnica ETSI TS 101 903 para XAdES ([3]) e em conformidade com as especificações adicionais seguintes:

O ds:CanonicalizationMethod que especifica o algoritmo de canonicalização aplicado ao elemento SignedInfo antes de efectuados os cálculos da assinatura identifica apenas um dos algoritmos seguintes:

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

NÃO DEVERIAM ser utilizados outros algoritmos ou as versões «Com comentários» dos algoritmos acima referidos para criar a assinatura, mas DEVERIAM ser suportados para assegurar uma interoperabilidade mínima para efeitos de verificação da assinatura.

O MD5 (RFC 1321) NÃO DEVE ser usado como algoritmo digest. Os signatários são remetidos para a legislação nacional aplicável e, para efeitos das orientações, para a especificação técnica ETSI TS 102 176 ([4]) e o relatório ECRYPT2 D.SPA.x ([5]), onde encontrarão mais recomendações sobre algoritmos e parâmetros elegíveis para assinaturas electrónicas.

Só podem ser utilizadas as *transformadas* a seguir enumeradas:

Transformada de canonicalizações: Consultar as especificações relevantes acima indicadas;

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

Filtros:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): para efeitos de compatibilidade e conformidade com XMLDSig

Filtro XPath 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): que substituiu o XPath devido a problemas de eficácia

Transformada da assinatura envolvida (*Enveloped*): (http://www.w3.org/2000/09/xmldsig#enveloped-signature)

Transformada XSLT (style sheet).

O elemento ds:KeyInfo DEVE incluir o certificado digital X.509 v3 do signatário (ou seja, o seu valor e não apenas uma referência ao valor).

A propriedade da assinatura assinada do «SigningCertificate» DEVE incluir o valor digest (CertDigest) e o IssuerSerial do certificado do signatário guardado em ds:KeyInfo e o URI opcional no campo «SigningCertificate» NÃO DEVE ser usado.

Está presente a propriedade SigningTime da assinatura assinada e inclui o UTC expresso no formato xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

O elemento DataObjectFormat DEVE estar presente e incluir o sub-elemento MimeType.

Se as assinaturas utilizadas pelos Estados-Membros se basearem num certificado qualificado, os objectos PKI (cadeia de certificados, dados de validade, marca temporal) incluídos nas assinaturas podem ser confirmados, nos termos da Decisão 2009/767/CE da Comissão, através das listas aprovadas do Estado-Membro que controla ou acredita o PSC que emitiu o certificado do signatário.

O Quadro 1 resume as especificações que uma assinatura XAdES-BES/EPES deve cumprir para ser suportada tecnicamente pelo Estado-Membro destinatário.

([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]) A versão mais recente é D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), de 30 de Março de 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Quadro 1

XAdES - BES (EPES)		**Requisitos mínimos comuns**
(a especificação técnica ETSI TS 103 903 aplica-se com os seguintes elementos)		
O=Obrigatório; F=Facultativo; R=Recomendado; N=Não utilizado		
ds: Signature ID	O	
ds: SignedInfo	O	
ds: CanonicalizationMethod	O	*Todos os algoritmos seguintes DEVEM ser suportados para verificação da assinatura; a criação DEVERIA restringir-se a um destes:* *- 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* *NÃO DEVERIAM ser utilizados outros métodos ou versões "#WithComments" dos métodos acima referidos.*
ds: SignatureMethod	O	***Algoritmos:*** *Consultar legislação nacional aplicável e, para efeitos das orientações, ver a especificação técnica ETSI TS 102 176 e o relatório ECRYPT2 D.SPA.7 para mais recomendações.*
ds: Reference URI	O	Uma referência a cada objecto de dados original a assinar (os URI também podem apontar para objectos externos) + referência ao elemento SignedProperties
ds: Transforms	F	*As aplicações de verificação DEVEM suportar todas as transformadas seguintes, enquanto as aplicações de criação de assinaturas DEVERIAM limitar-se a utilizar as transformadas seguintes:* *- Transformadas de canonicalização: ver acima* *- Codificação Base64* *- XPath e XPath Filter 2.0* *- Transformada da assinatura envolvida (Enveloped)* *- Transformadas XSLT*
ds: DigestMethod	O	***Algoritmos:*** *Consultar legislação nacional aplicável e, para efeitos das orientações, ver a especificação técnica ETSI TS 102 176 e o relatório ECRYPT2 D.SPA.7 para mais recomendações.*
ds: DigestValue	O	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	O	
ds: KeyInfo	O	DEVE incluir o certificado X509 (a propriedade assinada do SigningCertificate DEVE conter o valor digest do certificado do signatário) RECOMENDA-SE que a cadeia de certificação do certificado do signatário seja fornecida como ajuda ao processo de validação (neste caso, DEVEM ser fornecidos certificados X.509).
ds: Object		
QualifyingProperties	O	
SignedProperties	O	O
SignedSignatureProperties	O	O
SigningTime	O	UTC (xsd: dateTime).
SigningCertificate	O	DEVE conter o valor digest do certificado do signatário guardado em ds:KeyInfo e o URI facultativo é omitido (As aplicações PODEM procurar/encontrar o certificado do signatário em ds:KeyInfo, com base na equivalência hash).
SignaturePolicyIdentifier	F	apenas para o formato EPES (e para formatos superiores construídos a partir do formato EPES)
Signature ProductionPlace	F	
SignerRole	F	
/SignedSignatureProperties		
SignedDataObjectProperties	F	
DataObjectFormat	O	Quando este campo é utilizado, as aplicações DEVEM assegurar que os objectos de dados são apresentados ao utilizador desta forma. Quando utilizado, DEVE ser usado um elemento-filho MimeType.
CommitmentTypeIndication	F	
AllDataObjectsTimeStamp	F	
IndividualDataObjectTimeStamp	F	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	F	
UnsignedSignatureProperties		
CounterSignature	F	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Tipos de assinatura - Agrupamento de ficheiros originais assinados e assinaturas		
SignatureEnveloped		Todos DEVEM ser suportados
SignatureEnveloping		
SignatureDetached		

SECÇÃO 2 – CAdES-BES/EPES

A assinatura cumpre as especificações para as assinaturas Cryptographic Message Syntax (CMS) ([1]).

A assinatura utiliza atributos de assinatura CAdES-BES (ou -EPES), como estabelecido na especificação técnica ETSI TS 101 733 para CAdES ([2]), e cumpre as especificações adicionais, indicadas no Quadro 2 seguinte.

Todos os atributos da CAdES incluídos nos cálculos de *hash* da marca temporal do ficheiro (ETSI TS 101 733 V1.8.1, Anexo K) DEVEM estar em código DER e os restantes podem ser em BER para simplificar o processamento da CAdES com uma única passagem.

O MD5 (RFC 1321) NÃO DEVE ser utilizado como um algoritmo digest. Os signatários são remetidos para a legislação nacional aplicável e, para efeitos das orientações, para a especificação técnica ETSI TS 102 176 ([3]) e o relatório ECRYPT2 D.SPA.x ([4]), onde encontrarão mais recomendações sobre algoritmos e parâmetros elegíveis para assinaturas electrónicas.

Os atributos assinados DEVEM incluir uma referência ao certificado digital X.509 v3 do signatário (RFC 5035) e o campo *SignedData.certificates* DEVE incluir o respectivo valor.

O atributo assinado SigningTime DEVE estar presente e DEVE incluir o UTC expresso tal como em http://tools.ietf.org/html/rfc5652#section-11.3.

O atributo assinado ContentType DEVE estar presente e contém dados de identificação (http://tools.ietf.org/html/rfc5652#section-4) em que o tipo de conteúdo de dados visa referir-se a cadeias de octetos arbitrários, como texto com codificação UTF-8 ou ZIP com sub-elemento MimeType.

Se as assinaturas utilizadas pelos Estados-Membros se basearem num certificado qualificado, os objectos PKI (cadeia de certificados, dados de validade, marca temporal) incluídos nas assinaturas podem ser confirmados, nos termos da Decisão 2009/767/CE da Comissão, através das listas aprovadas do Estado-Membro que controla ou acredita o PSC que emitiu o certificado do signatário.

([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]) A versão mais recente é D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), de 30 de Março de 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Quadro 2

CAdES - BES (EPES)		**Requisitos mínimos comuns**
(a especificação técnica ETSI TS 101 733 aplica-se com os seguintes elementos)		
ASN.1		
`ContentInfo ::= SEQUENCE {`		
`contentType ContentType, -- id-signedData`		
`content [0] EXPLICIT ANY DEFINED BY contentType }`		
O=Obrigatório; F=Facultativo; R=Recomendado; N=Não utilizado		
`SignedData ::= SEQUENCE {`		
`version CMSVersion,`		
`digestAlgorithms DigestAlgorithmIdentifiers,`	O	**Algoritmos**: Consultar legislação nacional aplicável e, para efeitos das orientações, ver a especificação técnica ETSI TS 102 176 e o relatório ECRYPT2 D.SPA.7 para mais recomendações.
`encapContentInfo SEQUENCE {`		
`eContentType ContentType,`	O	id-Data
`eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },`	O/N	O atributo assinado ContentType está presente e contém dados de identificação (http://tools.ietf.org/html/rfc5652#section-4) em que o tipo de conteúdo de dados visa referir-se a cadeias de octetos arbitrários, como texto com codificação UTF-8 ou ZIP com sub-elemento MimeType
`-- External Data (if signature detached)*`		se assinatura isolada (detached), caso contrário não está presente. * Por dados externos entende-se dados protegidos por uma assinatura isolada que não estejam incluídos no conteúdo electrónico da assinatura CAdES. Recomenda-se a inclusão dos dados externos assinados juntamente com a assinatura no ficheiro ZIP.
`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	O	DEVE incluir certificado X509 do signatário. RECOMENDA-SE a inclusão de certificados de toda a cadeia de certificação até uma "âncora" de confiança.
`crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,`	F	
`signerInfos SET OF`	O	Pelo menos um signerInfo
`SEQUENCE { -- SignerInfo`		
`version CMSVersion,`		
`sid SignerIdentifier,`	F	(Valor não protegido)
`digestAlgorithm DigestAlgorithmIdentifier,`	O	**Algoritmos**: Consultar legislação nacional aplicável e, para efeitos das orientações, ver a especificação técnica ETSI TS 102 176 e o relatório ECRYPT2 D.SPA.7 para mais recomendações.
`signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF`		
`SEQUENCE { -- Attribute`	O	
`attrType OBJECT IDENTIFIER,`	O/F	**OBRIGATÓRIO**: id-contentType (com dados de id) id-messageDigest id-aa-ets-signingCertificateV2 ou id-aa-signingCertificate OBRIGATÓRIO: signingTime **FACULTATIVO**: id-aa-ets-sigPolicyId Outros atributos facultativos, como referido na especificação técnica ETSI TS 101 733.
`attrValues SET OF AttributeValue } OPTIONAL,`		
`signatureAlgorithm SignatureAlgorithmIdentifier,`		**Algoritmos**: Consultar legislação nacional aplicável e, para efeitos das orientações, ver a especificação técnica ETSI TS 102 176 e o relatório ECRYPT2 D.SPA.7 para mais recomendações.
`signature OCTET STRING, -- SignatureValue`		
`unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF`	F	
`SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }`	F	

SECÇÃO 3 – PAdES-PARTE 3 (BES/EPES):

A assinatura DEVE usar uma extensão de assinatura PAdES-BES (ou -EPES), de acordo com a especificação técnica ETSI TS 102 778, Parte 3, para PAdES ([1]) e cumpre as especificações adicionais seguintes:

O MD5 (RFC 1321) NÃO DEVE ser utilizado como um algoritmo digest. Os signatários são remetidos para a legislação nacional aplicável e, para efeitos das orientações, para a especificação técnica ETSI TS 102 176 ([2]) e o relatório ECRYPT2 D.SPA.x ([3]), onde encontrarão mais recomendações sobre algoritmos e parâmetros elegíveis para assinaturas electrónicas.

Os atributos assinados DEVEM incluir uma referência ao certificado digital X.509 v3 do signatário (RFC 5035) e o campo *SignedData.certificates* DEVE incluir o respectivo 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]) A versão mais recente é D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), de 30 de Março de 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

A hora da assinatura é indicada pelo valor na entrada **M** no dicionário da assinatura.

Se as assinaturas utilizadas pelos Estados-Membros se basearem num certificado qualificado, os objectos PKI (cadeia de certificados, dados de validade, marca temporal) incluídos nas assinaturas podem ser confirmados, nos termos da Decisão 2009/767/CE, através das listas aprovadas do Estado-Membro que controla ou acredita o PSC que emitiu o certificado do signatário.