DECIZII

DECIZIA COMISIEI

din 25 februarie 2011

de stabilire a unor cerințe minime pentru tratamentul transfrontalier al documentelor semnate electronic de autoritățile competente în temeiul Directivei 2006/123/CE a Parlamentului European și a Consiliului privind serviciile în cadrul pieței interne

[notificată cu numărul C(2011) 1081]

(Text cu relevanță pentru SEE)

(2011/130/UE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne [1], în special articolul 8 alineatul (3),

întrucât:

(1) Prestatorii de servicii ale căror servicii intră sub incidența Directivei 2006/123/CE trebuie să poată efectua, prin intermediul ghișeelor unice și prin mijloace electronice, procedurile și formalitățile necesare pentru a avea acces la activitățile lor și a le exercita. În limitele stabilite la articolul 5 alineatul (3) din Directiva 2006/123/CE, este posibil să mai existe cazuri în care prestatorii de servicii să fie obligați să prezinte documente originale, copii sau traduceri certificate atunci când efectuează astfel de proceduri și formalități. În astfel de cazuri, s-ar putea ca furnizorii de servicii să fie obligați să furnizeze documente semnate electronic de autoritățile competente.

(2) Utilizarea transfrontalieră a semnăturilor electronice avansate bazate pe certificate calificate este facilitată de Decizia 2009/767/CE a Comisiei din 16 octombrie 2009 de stabilire a unor măsuri de facilitare a utilizării procedurilor prin mijloace electronice prin intermediul ghișeelor unice în temeiul Directivei 2006/123/CE a Parlamentului European și a Consiliului privind serviciile în cadrul pieței interne [2] care, printre altele, impune statelor membre obligația de a efectua o evaluare a riscurilor înainte de a cere prestatorilor de servicii să utilizeze semnătura electronică și stabilește reguli de acceptare de către statele membre a semnăturilor electronice avansate bazate pe certificate calificate, create cu sau fără dispozitiv securizat de creare a semnăturii. Decizia 2009/767/CE nu tratează însă problema formatului semnăturilor electronice din documentele emise de autorități competente, care trebuie prezentate de prestatorii de servicii atunci când îndeplinesc procedurile și formalitățile necesare.

(3) Deoarece în momentul de față autoritățile competente din statele membre utilizează diverse forme de semnături electronice avansate pentru a semna electronic documentele (lor), statul membru destinatar care trebuie să proceseze aceste documente se poate confrunta cu dificultăți tehnice datorită diversității de semnături utilizate. Pentru a permite prestatorilor de servicii să efectueze procedurile și formalitățile transfrontaliere prin mijloace electronice, trebuie să se asigure capacitatea statelor membre de a procesa electronic cel puțin anumite semnături electronice atunci când primesc documente semnate electronic de autorități competente din alte state membre. Definirea unui anumit număr de formate de semnături electronice avansate pe care statele membre destinatare să fie obligate să le poată procesa electronic ar permite un grad mai mare de automatizare și ar îmbunătăți interoperabilitatea transfrontalieră a procedurilor electronice.

(4) S-ar putea ca statele membre ale căror autorități competente utilizează alte formate de semnături electronice decât cele utilizate în mod curent să fi implementat instrumente de validare care să permită și verificarea transfrontalieră a acestora. În astfel de cazuri, dacă informațiile necesare referitoare la instrumentele de validare nu sunt incluse direct în documentele electronice, în semnăturile electronice sau în suportul electronic al documentelor, este necesar ca ele să fie ușor accesibile pentru ca statul membru destinatar să poată utiliza respectivele instrumente.

(5) Prezenta decizie nu afectează modul în care statele membre definesc documentele originale, copiile și traducerile certificate. Obiectivul său se limitează la facilitarea verificării semnăturilor electronice în cazul în care sunt utilizate în documentele originale, copiile sau traducerile certificate pe care prestatorii de servicii ar putea fi obligați să le prezinte prin intermediul ghișeelor unice.

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

(6) Pentru a permite statelor membre să implementeze instrumentele tehnice necesare, prezenta decizie trebuie să se aplice de la 1 august 2011.

(7) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul Comitetului pe probleme referitoare la Directiva privind serviciile,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Formatul de referință al semnăturilor electronice

(1) Statele membre iau măsurile tehnice necesare care să le permită procesarea documentelor semnate electronic de autoritățile competente ale altor state membre cu o semnătură electronică avansată XML, CMS sau PDF în format BES sau EPES care respectă specificațiile tehnice din anexă, pe care prestatorii de servicii le prezintă în contextul efectuării de proceduri sau formalități prin intermediul ghișeelor unice, conform prevederilor de la articolul 8 din Directiva 2006/123/CE.

(2) Statele membre ale căror autorități competente semnează documentele menționate la alineatul (1) utilizând alte formate de semnătură electronică decât cele menționate la același alineat notifică Comisiei posibilitățile de validare existente care permit altor state membre să valideze online, gratuit și printr-o modalitate ușor de înțeles și pentru persoanele care nu sunt vorbitori nativi ai limbii respective, semnăturile electronice primite, în cazul în care informațiile necesare referitoare la instrumentele de validare nu sunt incluse direct în documentele electronice, în semnăturile electronice sau în suportul electronic al documentelor. Comisia va pune informațiile respective la dispoziția tuturor statelor membre.

Articolul 2

Aplicare

Prezenta decizie se aplică de la 1 august 2011.

Articolul 3

Destinatari

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 25 februarie 2011.

Pentru Comisie
Michel BARNIER
Membru al Comisiei

ANEXĂ

Specificații pentru semnăturile tehnice avansate de tip XML, CMS sau PDF care trebuie să poată fi procesate electronic de către statul membru destinatar

În următoarea secțiune a documentului, cuvintele-cheie „TREBUIE" (din engleză MUST), „NU TREBUIE" (din engleză MUST NOT), „OBLIGATORIU" (din engleză REQUIRED), „TREBUIE/NU TREBUIE" (din engleză SHALL/SHALL NOT), „AR TREBUI" (din engleză SHOULD), „NU AR TREBUI" (din engleză SHOULD NOT), „SE RECOMANDĂ" (din engleză RECOMMENDED), „ESTE POSIBIL" sau „POATE" (din engleză (MAY) și „OPȚIONAL" (din engleză OPTIONAL) și variantele lor gramaticale trebuie interpretate în sensul echivalentelor lor din limba engleză, în conformitate cu RFC 2119 ([1]).

SECȚIUNEA 1 – XadES-BES/EPES

Semnătura este conformă cu specificațiile pentru semnături W3C XML ([2])

Semnătura TREBUIE să fie cel puțin o semnătură de forma XAdES-BES (sau -EPES), conform specificațiilor ETSI TS 101 903 XAdES ([3]) și respectă toate specificațiile suplimentare următoare:

Metoda ds:CanonicalizationMethod care precizează algoritmul de punere în formă canonică aplicat elementului SignedInfo înainte de calcularea semnăturii identifică unul și numai unul din următorii algoritmi:

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#

Alți algoritmi și versiunile „With Comments" ale algoritmilor enumerați mai sus NU AR TREBUI utilizați pentru crearea semnăturii, dar AR TREBUI ca sistemul să îi poată procesa pentru interoperabilitatea reziduală a verificării semnăturilor.

MD5 (RFC 1321) NU TREBUIE utilizat ca digest algorithm. Semnatarii sunt invitați să consulte legislațiile naționale aplicabile, pentru linii directoare ETSI TS 102 176 ([4]), iar pentru recomandări suplimentare referitoare la algoritmii și parametrii eligibili pentru semnăturile electronice raportul ECRYPT2 D.SPA.x ([5]).

Utilizarea de *transforms* este limitată la lista de mai jos:

Canonicalization transforms: a se vedea specificațiile aferente de mai jos;

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

Filtrare:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): din motive de compatibilitate și conformitate cu XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): ca succesor al XPath datorită unor probleme de performanță

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

XSLT (style sheet) **transform**.

Elementul ds:KeyInfo TREBUIE să conțină certificatul digital X.509 v3 al semnatarului (mai precis valoarea acestuia, și nu o doar o trimitere la acesta).

Atributul „SigningCertificate" al semnăturii semnate TREBUIE să conțină valoarea digest (CertDigest) și IssuerSerial al certificatului semnatarului stocat în ds:KeyInfo, iar URI-ul opțional din câmpul „SigningCertificate" NU TREBUIE utilizat.

Atributul „*SigningTime*" al semnăturii semnate este prezent și conține UTC-ul exprimat ca xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

Elementul DataObjectFormat TREBUIE SĂ FIE prezent și conține subelementul MimeType.

În cazul în care semnăturile utilizate de statele membre se bazează pe un certificat calificat, obiectele PKI (lanțuri de certificate, date de revocare, marcaj de timp) incluse în semnături pot fi verificate utilizând lista sigură, conform Deciziei 2009/767/CE, a statului membru care supervizează sau acreditează CSP-ul care a emis certificatul semnatarului.

Tabelul 1 rezumă specificațiile pe care trebuie să le respecte o semnătură XAdES-BES/EPES pentru a putea fi procesată de sistemul informatic al statului membru destinatar.

([1]) IETF RFC 2119: „*Key words for use in RFCs to indicate Requirements Levels*".
([2]) W3C, XML Signature Syntax and Processing, (Versiunea 1.1), http://www.w3.org/TR/xmldsig-core1/.
W3C, XML Signature Syntax and Processing, (A doua ediție), 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; Partea 1: Hash functions and asymmetric algorithms; Partea 2: „Secure channel protocols and algorithms for signature creation devices".
([5]) Ultima versiune este D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), din 30 martie 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf)

Tabelul 1

XAdES - BES (EPES)		**Cerințe minime comune**
(ETSI TS 103 903 se aplică cu următoarele elemente profilate)		
M=Obligatoriu; O=Opțional; R=Recomandat; N=Neutilizat		
ds: Signature ID	M	
ds: SignedInfo	M	
ds: CanonicalizationMethod	M	*Toți algoritmii următori TREBUIE să poată fi procesați pentru verificarea semnăturii, crearea TREBUIE restricționată la unul din următoarele:* *- 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* *NU TREBUIE utilizate alte metode sau versiuni "#WithComments" ale metodelor menționate mai sus.*
ds: SignatureMethod	M	***Algoritmi:*** *consultați legislația națională aplicabilă, pentru linii directoare consultați ETSI TS 102 176, iar pentru recomandări suplimentare raportul ECRYPT2 D.SPA.7.*
ds: Reference URI	M	Otrimitere la fiecare obiect care trebuie semnat (URI-urile pot face trimitere și la obiecte externe), + trimitere la elementul SignedProperties
ds: Transforms	O	A*plicațiile de verificare TREBUIE să fie compatibile cu toți transforms de mai jos, în timp ce aplicațiile de creare a semnăturii TREBUIE să restricționeze utilizarea acestor transforms la următorii:* *- Canonicalization transforms: a se vedea mai jos* *- Base64 encoding* *- XPath and XPath Filter 2.0* *- Enveloped signature transform* *- XSLT transforms*
ds: DigestMethod	M	***Algoritmi:*** *consultați legislația națională aplicabilă, pentru linii directoare consultați ETSI TS 102 176, iar pentru recomandări suplimentare raportul ECRYPT2 D.SPA.7.*
ds: DigestValue	M	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	M	
ds: KeyInfo	M	TREBUIE să conțină certificatul X509 certificate (Atributul "SigningCertificate" al semnăturii semnate TREBUIE să conțină valoarea digest a certificatului semnatarului) Se RECOMANDĂ ca lanțurile de certificare a certificatelor semnatarului să fie furnizate ca indicație pentru a facilita procesul de validare (în acest caz TREBUIE furnizate certificatele X.509).
ds: Object		
QualifyingProperties	M	
SignedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC (xsd: dateTime).
SigningCertificate	M	TREBUIE să conțină valoarea digest a certificatului semnatarului stocat în ds:KeyInfo,iar URI optional se omite (Aplicațiile pot căuta/găsi certificatul semnatarului în ds:KeyInfo pe baza echivalenței hash).
SignaturePolicyIdentifier	O	doar pentru formatul EPES (și pentru formate superioare obținute pornind de la formatul EPES)
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	M	Când se completează acest câmp aplicațiile TREBUIE să asigure că obiectele sunt arătate utilizatorului în mod corespunzător. Atunci când se utilizează, TREBUIE utilizat un subelement MimeType.
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		Totul TREBUIE să poată fi procesat
SignatureEnveloping		
SignatureDetached		

SECȚIUNEA 2 – CAdES-BES/EPES

Semnătura este conformă cu specificațiile pentru semnături Cryptographic Message Syntax (CMS) [1].

Semnătura utilizează atribute CAdES-BES (sau -EPES) ale semnăturii, conform specificațiilor ETSI TS 101 733 CAdES [2], și respectă specificațiile suplimentare din tabelul 2 de mai jos.

Toate atributele CAdES incluse în calcul archive timestamp hash [(ETSI TS 101 733 V1.8.1 Anexa K) TREBUIE să fie criptate în DER, celelalte pot fi în BER pentru a simplifica procesul CAdES într-o singură trecere.

MD5 (RFC 1321) NU TREBUIE utilizat ca digest algorithm. Semnatarii sunt invitați să ia în considerare legislațiile naționale aplicabile, ca linii directoare, ETSI TS 102 176 [3] și raportul ECRYPT2 D.SPA.x [4] pentru recomandări suplimentare referitoare la algoritmii și parametrii eligibili pentru semnăturile electronice.

Atributele semnate TREBUIE să conțină o trimitere la certificatul digital X.509 v3 al semnatarului (RFC 5035), iar câmpul *SignedData.certificates* TREBUIE să conțină valoarea sa.

Atributul semnat SigningTime TREBUIE să fie prezent și TREBUIE să conțină UTC-ul conform cu http://tools.ietf.org/html/rfc5652#section-11.3.

Atributul semnat ContentType TREBUIE să fie prezent și conține id-data (http://tools.ietf.org/html/rfc5652#section-4), tipul de conținut al datelor servind ca referință la lanțuri de octeți arbitrari, cum ar fi text UTF-8 sau un ZIP container cu un subelement MimeType.

În cazul în care semnăturile utilizate de statele membre se bazează pe un certificat calificat, obiectele PKI (lanțuri de certificate, date de revocare, marcaj de timp) incluse în semnătură pot fi verificate utilizând lista sigură, conform Deciziei 2009/767/CE a Comisiei, a statului membru care supervizează sau acreditează CSP-ul care a emis certificatul semnatarului.

[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; Partea 1: Hash functions and asymmetric algorithms; Partea 2: „Secure channel protocols and algorithms for signature creation devices".

[4] Ultima versiune este D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), din 30 martie 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf)

Tabelul 2

CAdES - BES (EPES)		**Cerințe minime comune**
(ETSI TS 101 733 .....)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
M=Obligatoriu; O=Opțional; R=Recomandat; N=Neutilizat		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	M	***Algoritmi:*** *consultați legislația națională aplicabilă, pentru linii directoare consultați ETSI TS 102 176, iar pentru recomandări suplimentare raportul ECRYPT2 D.SPA.7.*
encapContentInfo SEQUENCE {		
eContentType ContentType,	M	id-Data
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached),	M/N	Atributul semnat ContentType este prezent și conține id-data (http://tools.ietf.org/html/rfc5652#section-4) în cazul în care conținutul de date se referă la lanțuri de octeți arbitrari, precum text UTF-8 text sau ZIP container cu subelement MimeType
-- External Data (if signature detached)*		în caz de semnătură despărțită, altfel nu este prezent. * Date externe înseamnă date protejate printr-o semnătură despărțită care nu este inclusă în eConținutul semnăturii CAdES. Se recomandă includerea datelor externe semnate împreună cu semnătura într-un fișier ZIP.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	M	TREBUIE să conțină un certificat X509 de la semnatar. Se recomandă includerea certificatelor din întregul lanț de certificare până la un punct de încredere.
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	O	
signerInfos SET OF	M	Cel puțin un signerInfo
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	O	(Valoare neprotejată)
digestAlgorithm DigestAlgorithmIdentifier,	M	***Algoritmi:*** *consultați legislația națională aplicabilă, pentru linii directoare consultați ETSI TS 102 176, iar pentru recomandări suplimentare raportul ECRYPT2 D.SPA.7.*
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	M	
attrType OBJECT IDENTIFIER,	M/O	**OBLIGATORIU:** id-contentType (cu id data) id-messageDigest id-aa-ets-signingCertificateV2 sau id-aa-signingCertificate OBLIGATORIU: signingTime **OPTIONAL**: id-aa-ets-sigPolicyId Alte atribute opționale sunt definite în ETSI TS 101 733.
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		***Algoritmi:*** *consultați legislația națională aplicabilă, pentru linii directoare consultați ETSI TS 102 176, iar pentru recomandări suplimentare raportul ECRYPT2 D.SPA.7.*
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	O	
SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }	O	

SECȚIUNEA 3 – PAdES-PART 3 (BES/EPES)

Semnătura TREBUIE să utilizeze o extensie a semnăturii de forma PAdES-BES (sau -EPES), conform specificațiilor ETSI TS 102 778 PAdES partea 3 ([1]), și respectă specificațiile suplimentare următoare:

MD5 (RFC 1321) NU TREBUIE utilizat ca digest algorithm. Semnatarii sunt invitați să ia în considerare legislațiile naționale aplicabile, ca linii directoare, ETSI TS 102 176 ([2]) și raportul ECRYPT2 D.SPA.x ([3]) pentru recomandări suplimentare referitoare la algoritmii și parametrii eligibili pentru semnăturile electronice.

Atributele semnate TREBUIE să conțină o trimitere la certificatul digital X.509 v3 al semnatarului (RFC 5035), iar câmpul *SignedData.certificates* trebuie să conțină valoarea sa.

([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; Partea 1: Hash functions and asymmetric algorithms; Partea 2: „Secure channel protocols and algorithms for signature creation devices".

([3]) Ultima versiune este D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), din 30 martie 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf)

Momentul semnării este indicat de valoarea intrării **M** în dicționarul de semnătură.

În cazul în care semnăturile utilizate de statele membre se bazează pe un certificat calificat, obiectele PKI (lanțuri de certificate, date de revocare, marcaj de timp) incluse în semnătură pot fi verificate utilizând lista sigură, conform Deciziei 2009/767/CE, a statului membru care supervizează sau acreditează CSP-ul care a emis certificatul semnatarului.