LĒMUMI

KOMISIJAS LĒMUMS

(2011. gada 25. februāris),

ar kuru nosaka minimālās prasības kompetento iestāžu elektroniski parakstītu dokumentu pārrobežu apstrādei saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 2006/123/EK par pakalpojumiem iekšējā tirgū

(izziņots ar dokumenta numuru C(2011) 1081)

(Dokuments attiecas uz EEZ)

(2011/130/ES)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2006. gada 12. decembra Direktīvu 2006/123/EK par pakalpojumiem iekšējā tirgū [1] un jo īpaši tās 8. panta 3. punktu,

tā kā:

(1) Pakalpojumu sniedzējiem, uz kuru sniegtajiem pakalpojumiem attiecas Direktīva 2006/123/EK, jāspēj ar vienoto kontaktpunktu starpniecību un elektroniskā formā izpildīt pakalpojumu piekļuvei un sniegšanai vajadzīgās procedūras un formalitātes. Ievērojot Direktīvas 2006/123/EK 5. panta 3. punktā noteiktos ierobežojumus, var būt gadījumi, kad pakalpojumu sniedzējiem minēto procedūru un formalitāšu izpildei jāiesniedz dokumentu oriģināli, apliecinātas kopijas vai apstiprināti tulkojumi. Šajos gadījumos pakalpojumu sniedzējiem var rasties nepieciešamība iesniegt kompetento iestāžu elektroniski parakstītus dokumentus.

(2) Uz kvalificētu sertifikātu balstītu uzlabotu elektronisko parakstu pārrobežu izmantošanu veicina Komisijas 2009. gada 16. oktobra Lēmums 2009/767/EK par pasākumiem, lai veicinātu procedūru veikšanu elektroniski, izmantojot vienotos kontaktpunktus atbilstoši Eiropas Parlamenta un Padomes Direktīvai 2006/123/EK par pakalpojumiem iekšējā tirgū [2], kas, *inter alia*, paredz dalībvalstīm veikt risku novērtējumu, pirms no pakalpojumu sniedzējiem prasīt šādus elektroniskos parakstus, kā arī paredz noteikumus, kas dalībvalstīm jāievēro, pieņemot uz kvalificētu sertifikātu balstītus uzlabotus elektroniskos parakstus, kas izveidoti ar drošu paraksta radīšanas ierīci vai bez tās. Taču Lēmums 2009/767/EK neattiecas uz elektroniskā paraksta formātiem kompetento iestāžu izsniegtajos dokumentos, kas pakalpojumu sniedzējiem jāiesniedz, izpildot vajadzīgās procedūras un formalitātes.

(3) Tā kā dalībvalstu kompetentās iestādes dokumentu parakstīšanai elektroniski pašlaik izmanto dažādus uzlabotu elektronisko parakstu formātus, tad saņēmējas dalībvalstis, kam jāapstrādā šie dokumenti, dažādo elektronisko parakstu formātu dēļ var saskarties ar tehniskiem sarežģījumiem. Lai nodrošinātu iespēju pakalpojumu sniedzējiem izpildīt pārrobežu procedūras un formalitātes elektroniski, ir jāgarantē, ka dalībvalstis spēj atbalstīt vismaz daļu uzlabotu elektronisko parakstu formātu tad, kad tās saņem elektroniski parakstītus dokumentus no citu dalībvalstu kompetentajām iestādēm. Automatizāciju palielinātu un elektronisko procedūru pārrobežu savietojamību uzlabotu to elektronisko parakstu formātu noteikšana, kuru tehniskais atbalsts nepieciešams dalībvalstī, kas saņem dokumentu.

(4) Iespējams, ka dalībvalstis, kuru kompetentās iestādes nelieto visplašāk tehniski atbalstītos elektroniskā paraksta formātus, ir ieviesušas veidus, kā to parakstus verificēt arī pārrobežu mērogā. Lai minētajā gadījumā saņēmējas dalībvalstis varētu paļauties uz šiem validācijas līdzekļiem, informācija par tiem ir jāpadara viegli pieejama, ja vien vajadzīgā informācija nav jau iekļauta pašos elektroniskajos dokumentos, elektroniskajos parakstos vai elektroniskajos dokumentu nesējos.

(5) Šis lēmums neietekmē dalībvalstu novērtējumu par to, ko saprot ar dokumenta oriģinālu, apliecinātu kopiju vai apstiprinātu tulkojumu. Lēmuma mērķis ir tikai atvieglot elektronisko parakstu verifikāciju, ja tie lietoti to dokumentu oriģinālos, apliecinātās kopijās vai apstiprinātos tulkojumos, ko pakalpojumu sniedzēji iesniedz ar vienoto kontaktpunktu starpniecību.

[1] OV L 376, 27.12.2006., 36. lpp.
[2] OV L 274, 20.10.2009., 36. lpp.

(6) Lai ļautu dalībvalstīm ieviest vajadzīgos tehniskos līdzekļus, ir pamatoti, ka šo lēmumu piemēro no 2011. gada 1. augusta.

(7) Šajā lēmumā paredzētie pasākumi ir saskaņā ar Pakalpojumu direktīvas komitejas atzinumu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Elektronisko parakstu standartformāts

1. Dalībvalstis ievieš vajadzīgos tehniskos līdzekļus to elektroniski parakstīto dokumentu apstrādei, kurus pakalpojumu sniedzēji iesniedz ar vienoto kontaktpunktu starpniecību, lai izpildītu procedūras un formalitātes, kas noteiktas Direktīvas 2006/123/EK 8. pantā, un kurus citu valstu kompetentās iestādes parakstījušas ar uzlabotu *XML*, *CMS* vai *PDF* elektronisko parakstu *BES* vai *EPES* formātā, kas atbilst pielikumā uzskaitītajiem tehniskajiem parametriem.

2. Dalībvalstis, kuru kompetentās iestādes paraksta 1. punktā minētos dokumentus, izmantojot elektroniskā paraksta formātus, kas nav minēti tajā pašā punktā, informē Komisiju par esošajām iespējām, kas ļauj citām dalībvalstīm tiešsaistē, bez maksas un veidā, kas saprotams personām, kam attiecīgā valoda nav dzimtā valoda, validēt saņemtos elektroniskos parakstus, ja vien vajadzīgā informācija nav jau iekļauta pašos elektroniskajos dokumentos, elektroniskajos parakstos vai elektroniskajos dokumentu nesējos. Komisija šo informāciju dara pieejamu dalībvalstīm.

2. pants

Piemērošana

Šo lēmumu piemēro no 2011. gada 1. augusta.

3. pants

Adresāti

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2011. gada 25. februārī

Komisijas vārdā –
Komisijas loceklis
Michel BARNIER

PIELIKUMS

Specifikācijas *XML, CMS* vai *PDF* formāta uzlabota elektroniskā paraksta tehniskajam atbalstam saņēmējā dalībvalstī

Turpmākajā dokumenta daļā lietotā vajadzības un aizlieguma izteiksme, īstenības un nolieguma izteiksme, nosacījuma izteiksme un atslēgvārdi "IETEICAMS", "VAR" un "PĒC IZVĒLES" jāinterpretē tā, kā izklāstīts *RFC 2119* [1].

1. IEDAĻA – *XAdES-BES/EPES*

Šis paraksts atbilst *W3C XML* paraksta specifikācijām [2].

Šim parakstam JĀBŪT vismaz *XAdES-BES* (vai *-EPES*) paraksta formātā, kā norādīts *ETSI TS 101 903 XAdES* specifikācijās [3], un tas atbilst visām sekojošām papildu specifikācijām.

Elements *ds:CanonicalizationMethod*, kas norāda kanonizācijas algoritmu, kuru piemēro *SignedInfo* elementam, pirms izdarīt paraksta aprēķinus, identificē tikai vienu no sekojošajiem algoritmiem:

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#

Citus algoritmus vai iepriekš minēto algoritmu versijas "*With comments*" NEVAJADZĒTU lietot parakstu radīšanā, bet tie BŪTU jāatbalsta, lai veiktu parakstu verifikāciju atlikušo savietojamības vajadzību ietvaros.

MD5 (*RFC 1321*) NEDRĪKST lietot ka īssavilkuma algoritmu. Parakstītāji tiek aicināti sīkāku informāciju meklēt attiecīgajos valstu tiesību aktos, vadlīnijas meklējamas *ETSI TS 102 176* [4], un turpmāki ieteikumi par elektroniskajos parakstos izmantojamajiem algoritmiem un parametriem atrodami *ECRYPT2 D.SPA.x* [5] ziņojumā.

Pārveidojumiem (*transforms*) izmanto tikai vienu no turpmāk minētajiem.

Kanonizācijas pārveidojumi: skatīt minētās specifikācijas

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

Filtrēšana:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): savietojamības nolūkos un atbilstībai *XMLDSig*

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): *XPath* vietā veiktspējas problēmu dēļ

Iegultā (*enveloped*) paraksta pārveidojums: (http://www.w3.org/2000/09/xmldsig#enveloped-signature)

XSLT (stila lapa) **pārveidojums**

Elementam *ds:KeyInfo* JĀIETVER parakstītāja *X.509 v3* digitālais sertifikāts (t. i., ne tikai atsauce uz to, bet tā vērtība).

Ar "*SigningCertificate*" parakstītam parakstam JĀSATUR īssavilkuma vērtība (*CertDigest*) un *IssuerSerial* parakstītāja sertifikāts, kas tiek saglabāts *ds:KeyInfo*, un neobligāto *URI "SigningCertificate*" laukā lietot NEDRĪKST.

Parakstīta paraksta *SigningTime* atribūts ir norādīts un satur *UTC*, kas izteikts kā *xsd:dateTime* (http://www.w3.org/TR/xmlschema-2/#dateTime).

DataObjectFormat elementam ir JĀBŪT norādītam, un tam jāsatur *MimeType* apakšelements.

Ja dalībvalstu lietotie paraksti ir balstīti uz kvalificētu sertifikātu, tad parakstos iekļautie *PKI* objekti (sertificēšanas ķēdes, atsaukšanas dati, laika zīmogi) ir verificējami saskaņā ar Komisijas Lēmumu 2009/767/EK, izmantojot uzticamo sarakstu tajā dalībvalstī, kas uzrauga vai akreditē to SPS, kas izsniedzis parakstītāja sertifikātu.

1. tabulā norādītas specifikācijas, kuras jāievēro, lai *XAdES-BES/EPES* parakstu tehniski atbalstītu saņēmējas dalībvalstis.

---

[1] *IETF RFC 2119*: "*Key words for use in RFCs to indicate Requirements Levels*".

[2] *W3C, XML Signature Syntax and Processing* (1.1. versija), http://www.w3.org/TR/xmldsig-core1/.
W3C, XML Signature Syntax and Processing (otrā redakcija), 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;* 1. daļa: *Hash functions and asymmetric algorithms;* 2. daļa: *Secure channel protocols and algorithms for signature creation devices.*

[5] Jaunākā versija ir *D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), dated 30 March 2010* (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

1. tabula

XAdES - BES (EPES)		**Vienotas minimālās prasības**
(ETSI TS 103 903 piemēro ar šādiem profila elementiem)		
O = obligāti; P = pēc izvēles; I = ieteicams; N = nelieto		
ds: Signature ID	**O**	
ds: SignedInfo	**O**	
ds: CanonicalizationMethod	**O**	***Visi sekojošie algoritmi JĀATBALSTA parakstu verifikācijas vajadzībām, parakstu veidošanā BŪTU jāizmanto tikai viens no šiem:*** ***- 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*** ***Citas metodes vai minēto metožu versijas "#WithComments" NEVAJADZĒTU lietot.***
ds: SignatureMethod	**O**	***Algoritmi: sīkāka informācija attiecīgajos valstu tiesību aktos, vadlīnijas meklējamas ETSI TS 102 176, un turpmāki ieteikumi atrodami ECRYPT2 D.SPA.7 ziņojumā.***
ds: Reference URI	**O**	**Viena atsauce uz katru parakstāmo oriģinālo datu objektu (*URI* var norādīt arī uz ārēju objektu), + atsauce uz *SignedProperties* elementu**
ds: Transforms	**P**	***Verifikācijas lietojumprogrammām JĀATBALSTA visi sekojošie pārveidojumi, bet parakstu veidošanā lietojumprogrammām BŪTU jāizmanto tikai viens no šiem pārveidojumiem (transforms):*** ***- Kanonizācijas pārveidojumi: skatīt iepriekš*** ***- Base64 kodējums*** ***- XPath un XPath Filter 2.0*** ***- Iegultā (enveloped) paraksta pārveidojums*** ***- XSLT pārveidojums***
ds: DigestMethod	**O**	***Algoritmi: sīkāka informācija attiecīgajos valstu tiesību aktos, vadlīnijas meklējamas ETSI TS 102 176, un turpmāki ieteikumi atrodami ECRYPT2 D.SPA.7 ziņojumā.***
ds: DigestValue	**O**	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	**O**	
ds: KeyInfo	**O**	**JĀSATUR X509 sertifikāts (*SigningCertificate* parakstītajam atribūtam JĀSATUR parakstītāja sertifikāta īssavilkuma vērtība)** **Lai veicinātu validēšanas procesu, IETEICAMS norādīt parakstītāja sertifikāta sertificēšanas ķēdi (šādā gadījumā JĀPIEVIENO X.509 sertifikāts).**
ds: Object		
QualifyingProperties	**O**	
SignedProperties	**O**	**M**
SignedSignatureProperties	**O**	**M**
SigningTime	**O**	**UTC (xsd: dateTime).**
SigningCertificate	**O**	**JĀSATUR *ds:KeyInfo* saglabātā parakstītāja sertifikāta īssavilkuma vērtība, izlaižot neobligāto *URI* vērtību (lietojumprogrammas VAR uz jaucējekvivalences bāzes meklēt/atrast parakstītāja sertifikātu *ds:KeyInfo*)**
SignaturePolicyIdentifier	**P**	**tikai *EPES* formātam (un citiem formātiem, kas balstīti uz *EPES*)**
Signature ProductionPlace	**P**	
SignerRole	**P**	
/SignedSignatureProperties		
SignedDataObjectProperties	**P**	
DataObjectFormat	**O**	**Ja izmanto šo lauku, lietojumprogrammām jānodrošina datu objektu pienācīgs atveidojums lietotājam.** **Ja to izmanto, JĀIZMANTO *MimeType* bērnelements.**
CommitmentTypeIndication	**P**	
AllDataObjectsTimeStamp	**P**	
IndividualDataObjectTimeStamp	**P**	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	**P**	
UnsignedSignatureProperties		
CounterSignature	**P**	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Signature topology - Packaging signed original files and signatures		
SignatureEnveloped		**JĀATBALSTA visi**
SignatureEnveloping		
SignatureDetached		

2. IEDAĻA – *CAdES-BES/EPES*

Šis paraksts atbilst *Cryptographic Message Syntax* (*CMS*) paraksta specifikācijām ([1]).

Parakstā izmantoti *CAdES-BES* (vai *-EPES*) paraksta atribūti, kā noteikts *ETSI TS 101 733 CAdES* specifikācijās ([2]), un paraksts atbilst 2. tabulā norādītajām specifikācijām.

Visiem *CAdES* atribūtiem, kas iekļauti arhivēto laika zīmogu jaucējaprēķinos (*ETSI TS 101 733* V1.8.1 pielikums K), JĀBŪT *DER* kodējumā, visi pārējie var būt *BER*, lai vienkāršotu *CAdES* vienpārejas apstrādi.

MD5 (*RFC 1321*) NEDRĪKST lietot ka īssavilkuma algoritmu. Parakstītāji tiek aicināti sīkāku informāciju meklēt attiecīgajos valstu tiesību aktos, vadlīnijas meklējamas *ETSI TS 102 176* ([3]), un turpmāki ieteikumi par elektroniskajos parakstos izmantojamajiem algoritmiem un parametriem atrodami *ECRYPT2 D.SPA.x* ([4]) ziņojumā.

Parakstītajos atribūtos JĀBŪT iekļautai atsaucei uz parakstītāja *X.509 v3* digitālo sertifikātu (*RFC 5035*), un *SignedData.-certificates* laukā JĀNORĀDA tā vērtība.

SigningTime parakstītajam atribūtam ir JĀBŪT norādītam un tam JĀSATUR *UTC*, kas izteikts kā šeit: http://tools.ietf.org/html/rfc5652#section-11.3.

ContentType parakstītajam atribūtam ir JĀBŪT norādītam, un tas satur *id-data* (http://tools.ietf.org/html/rfc5652#section-4), kur datu satura veids attiecas uz brīvi izvēlētām oktetu virknēm, piemēram, *UTF-8* tekstu vai *ZIP* konteineru ar *MimeType* apakšelementu.

Ja dalībvalstu lietotie paraksti ir balstīti uz kvalificētu sertifikātu, tad parakstos iekļautie *PKI* objekti (sertificēšanas ķēdes, atsaukšanas dati, laika zīmogi) ir verificējami saskaņā ar Lēmumu 2009/767/EK, izmantojot uzticamo sarakstu tajā dalībvalstī, kas uzrauga vai akreditē to SPS, kas izsniedzis parakstītāja sertifikātu.

([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;* 1. daļa: *Hash functions and asymmetric algorithms;* 2. daļa: *Secure channel protocols and algorithms for signature creation devices.*

([4]) Jaunākā versija ir *D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes* (2009–2010), *dated 30 March 2010* (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

2. tabula

CAdES - BES (EPES)		**Vienotas minimālās prasības**
(ETSI TS 101 733 piemēro ar šādiem profila elementiem)		
ASN.1		
`ContentInfo ::= SEQUENCE {`		
`contentType ContentType, -- id-signedData`		
`content [0] EXPLICIT ANY DEFINED BY contentType }`		
O = obligāti; P = pēc izvēles; I = ieteicams; N = nelieto		
`SignedData ::= SEQUENCE {`		
`version CMSVersion,`		
`digestAlgorithms DigestAlgorithmIdentifiers,`	**O**	**Algoritmi: sīkāka informācija attiecīgajos valstu tiesību aktos, vadlīnijas meklējamas ETSI TS 102 176, un turpmāki ieteikumi atrodami ECRYPT2 D.SPA.7 ziņojumā.**
`encapContentInfo SEQUENCE {`		
`eContentType ContentType,`	**O**	**id-Data**
`eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },`	**O/N**	**ContentType parakstītais atribūts ir norādīts un satur *id-data* (http://tools.ietf.org/html/rfc5652#section-4), kur datu satura veids attiecas uz brīvi izvēlētām oktetu virknēm, piemēram, *UTF-8* tekstu vai *ZIP* konteineru ar *MimeType* apakšelementu**
`-- External Data (if signature detached)*`		**ja atdalītais paraksts nav citādi klātesošs. * Ārējie dati nozīmē datus, kas aizsargāti ar atdalīto parakstu, kas nav iekļauts *CAdES* paraksta e-saturā (*eContent*). Ir ieteicams pievienot *ZIP* datni, kas satur parakstītus ārējos datus kopā ar parakstu.**
`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	**O**	**JĀSATUR parakstītāja X509 sertifikāts. IETEICAMS iekļaut visus sertificēšanas ķēdes sertifikātus līdz pat drošības enkuram.**
`crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,`	**P**	
`signerInfos SET OF`	**O**	**Vismaz viens *signerInfo***
`SEQUENCE { -- SignerInfo`		
`version CMSVersion,`		
`sid SignerIdentifier,`	**P**	**(Neaizsargāta vērtība)**
`digestAlgorithm DigestAlgorithmIdentifier,`	**O**	**Algoritmi: sīkāka informācija attiecīgajos valstu tiesību aktos, vadlīnijas meklējamas ETSI TS 102 176, un turpmāki ieteikumi atrodami ECRYPT2 D.SPA.7 ziņojumā.**
`signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF`		
`SEQUENCE { -- Attribute`	**O**	
`attrType OBJECT IDENTIFIER,`	**O/P**	**OBLIGĀTI: id-contentType (ar id data) id-messageDigest id-aa-ets-signingCertificateV2 vai id-aa-signingCertificate OBLIGĀTI: signingTime PĒC IZVĒLES: id-aa-ets-sigPolicyId Citi izvēles atribūti, kā norādīts ETSI TS 101 733.**
`attrValues SET OF AttributeValue } OPTIONAL,`		
`signatureAlgorithm SignatureAlgorithmIdentifier,`		**Algoritmi: sīkāka informācija attiecīgajos valstu tiesību aktos, vadlīnijas meklējamas ETSI TS 102 176, un turpmāki ieteikumi atrodami ECRYPT2 D.SPA.7 ziņojumā.**
`signature OCTET STRING, -- SignatureValue`		
`unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF`	**P**	
`SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }`	**P**	

3. IEDAĻA – *PAdES*-3. DAĻA (*BES*/*EPES*)

Parakstā JĀLIETO *PAdES-BE* (vai -*EPES*) paraksta paplašinājums, kā norādīts *ETSI TS 102 778 PAdES*-3. daļas specifikācijās ([1]), un tas atbilst visām sekojošām papildu specifikācijām:

MD5 (*RFC 1321*) NEDRĪKST lietot kā īssavilkuma algoritmu. Parakstītāji tiek aicināti sīkāku informāciju meklēt attiecīgajos valstu tiesību aktos, vadlīnijas meklējamas *ETSI TS 102 176* ([2]), un turpmāki ieteikumi par elektroniskajos parakstos izmantojamajiem algoritmiem un parametriem atrodami *ECRYPT2 D.SPA.x* ([3]) ziņojumā.

Parakstītajos atribūtos JĀBŪT iekļautai atsaucei uz parakstītāja *X.509 v3* digitālo sertifikātu (*RFC 5035*) un *SignedData.-certificates* laukā JĀNORĀDA tā vērtība.

([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;* 1. daļa: *Hash functions and asymmetric algorithms;* 2. daļa: *Secure channel protocols and algorithms for signature creation devices.*

([3]) Jaunākā versija ir *D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), dated 30 March 2010* (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Parakstīšanas laiku norāda ar **M** šķirkļa vērtību paraksta vārdnīcā.

Ja dalībvalstu lietotie paraksti ir balstīti uz kvalificētu sertifikātu, tad parakstos iekļautie *PKI* objekti (sertificēšanas ķēdes, atsaukšanas dati, laika zīmogi) ir verificējami saskaņā ar Lēmumu 2009/767/EK, izmantojot uzticamo sarakstu tajā dalībvalstī, kas uzrauga vai akreditē to SPS, kas izsniedzis parakstītāja sertifikātu.