OTSUSED

KOMISJONI OTSUS,

25. veebruar 2011,

millega kehtestatakse pädevate asutuste poolt elektrooniliselt allkirjastatud dokumentide piiriülese töötlemise miinimumnõuded vastavalt Euroopa Parlamendi ja nõukogu direktiivile 2006/123/EÜ teenuste kohta siseturul

(teatavaks tehtud numbri K(2011) 1081 all)

(EMPs kohaldatav tekst)

(2011/130/EL)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 12. detsembri 2006. aasta direktiivi 2006/123/EÜ teenuste kohta siseturul, [1] eriti selle artiklit 8 lõiget 3,

ning arvestades järgmist:

(1) Teenuseosutajad, kelle teenused kuuluvad direktiivi 2006/123/EÜ reguleerimisalasse, peavad olema võimelised teostama ühtsete kontaktpunktide ja elektrooniliste vahendite kaudu menetlusi ja toiminguid, mis on vajalikud nende teenustele juurdepääsuks ja teenuste osutamiseks. Direktiivi 2006/123/EÜ artikli 5 lõike 3 kohaselt võib ikka veel esineda juhtumeid, kus teenuseosutaja peab esitama nende menetluste ja toimingute teostamisel originaaldokumente, tõestatud koopiaid või kinnitatud tõlkeid. Neil juhtudel võib teenuseosutajatel olla tarvis esitada dokumente, mille pädevad asutused on allkirjastanud elektrooniliselt.

(2) Kvalifitseeritud sertifikaadil põhinevate täiustatud elektrooniliste allkirjade piiriülest kasutamist on lihtsustatud komisjoni 16. oktoobri 2009. aasta otsusega 2009/767/EÜ, millega kehtestatakse meetmed elektrooniliste haldustoimingute kasutamise lihtsustamiseks ühtsete kontaktpunktide kaudu, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 2006/123/EÜ teenuste kohta siseturul, [2] millega seatakse liikmesriikidele muu hulgas kohustus viia enne teenuseosutajatelt elektrooniliste allkirjade nõudmist läbi riskianalüüs, ning kehtestatakse reeglid kvalifitseeritud sertifikaadil põhinevate, turvalise allkirja andmise vahendiga või ilma selleta genereeritud täiustatud elektrooniliste allkirjade vastuvõtmiseks liikmesriikide poolt. Samas ei käsitleta otsuses 2009/767/EÜ elektrooniliste allkirjade vorminguid nendes pädevate asutuste väljastatavates dokumentides, mille teenuseosutajad peavad vastavate menetluste ja toimingute teostamisel esitama.

(3) Kuna praegu kasutavad liikmesriikide pädevad asutused oma dokumentide elektrooniliseks allkirjastamiseks erinevaid täiustatud elektroonilise allkirja vorminguid, võib liikmesriikidel, kellele need dokumendid saadetakse ja kes peavad neid töötlema, tekkida kasutatavate allkirjavormingute erinevuse tõttu tehnilisi raskusi. Selleks et võimaldada teenuseosutajatel teostada oma menetlusi ja toiminguid piiriüleselt elektrooniliste vahendite kaudu, on vaja tagada, et liikmesriikide süsteemid toetaksid tehniliselt vähemalt teatavat hulka täiustatud elektroonilise allkirja vorminguid, kui neile saadetakse teiste liikmesriikide pädevate asutuste poolt elektrooniliselt allkirjastatud dokumente. Kui määratleda teatud hulk täiustatud elektroonilise allkirja vorminguid, mida saaja-liikmesriigi süsteemid peavad tehniliselt toetama, võimaldaks see ulatuslikumat automatiseerimist ja parandaks elektrooniliste menetluste piiriülest koostalitlusvõimet.

(4) On võimalik, et liikmesriigid, kelle pädevad asutused kasutavad muid elektroonilise allkirja vorminguid kui üldiselt toetatavad vormingud, on juurutanud verifitseerimisvahendid, mis võimaldavad nende allkirjade verifitseerimist ka piiriüleselt. Kui see on nii, on vaja teha teave nende verifitseerimisvahendite kohta kergesti ligipääsetaval viisil kättesaadavaks, et liikmesriigid, kellele dokumente saadetakse, saaksid neid vahendeid kasutada, välja arvatud juhul, kui vajalik teave sisaldub juba saadetavates elektroonilistes dokumentides, elektroonilistes allkirjades või elektrooniliste dokumentide kandjates.

(5) Käesolev otsus ei mõjuta liikmesriikide õigust määrata, mis kujutab endast originaali, mis tõestatud koopiat ja mis kinnitatud tõlget. Otsuse eesmärk on piiratud sellega, et lihtsustada elektrooniliste allkirjade verifitseerimist sel juhul, kui neid kasutatakse originaalidel, tõestatud koopiatel või kinnitatud tõlgetel, mille teenuseosutajad peavad ühtsete kontaktpunktide kaudu esitama.

[1] ELT L 376, 27.12.2006, lk 36.
[2] ELT L 274, 20.10.2009, lk 36.

(6) Võimaldamaks liikmesriikidel vajalikud tehnilised vahendid juurutada, on mõistlik, et seda otsust kohaldatakse alates 1. augustist 2011.

(7) Käesoleva otsusega ette nähtud meetmed on kooskõlas teenuste direktiivi komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Elektroonilise allkirja standardvormingud

1. Liikmesriigid juurutavad vajalikud tehnilised vahendid, mis võimaldavad neil töödelda elektrooniliselt allkirjastatud dokumente, mida teenuseosutajad ühtsete kontaktpunktide kaudu menetlusi ja toiminguid teostades esitavad, nagu ette nähtud direktiivi 2006/123/EÜ artikliga 8, ja mis on allkirjastatud teiste liikmesriikide pädevate asutuste poolt BES- või EPES-vormingus XMLi või CMSi või PDFi täiustatud elektrooniliste allkirjadega, mis vastavad lisas sätestatud tehnilistele kirjeldustele.

2. Liikmesriigid, kelle pädevates asutustes allkirjastatakse lõikes 1 osutatud dokumente, kasutades muid elektroonilise allkirja vorminguid kui samas lõikes osutatud vormingud, teavitavad komisjoni olemasolevatest verifitseerimisvõimalustest, mis võimaldavad teistel liikmesriikidel laekunud elektroonilisi allkirju interneti teel, tasuta ja kasutatud keelt emakeelena mittekõnelevale inimesele arusaadaval viisil verifitseerida, välja arvatud juhul, kui nõutav teave sisaldub juba saadetavas dokumendis, elektroonilises allkirjas või elektroonilises dokumendikandjas. Komisjon teeb selle teabe kättesaadavaks kõigile liikmesriikidele.

Artikkel 2

Kohaldamine

Käesolevat otsust kohaldatakse alates 1. augustist 2011.

Artikkel 3

Adressaadid

Käesolev otsus on adresseeritud liikmesriikidele.

Brüssel, 25. veebruar 2011

Komisjoni nimel
komisjoni liige
Michel BARNIER

LISA

XMLi, CMSi või PDFi täiustatud elektrooniliste allkirjade spetsifikaadid – elektroonilised allkirjad, mida saaja-liikmesriigi süsteemid peavad tehniliselt toetama

Dokumendi järgnevas osas tuleb võtmesõnu „PEAB”, „EI TOHI”, „NÕUTAV”, „TULEB”, „EI TULE”, „PEAKS”, „EI PEAKS”, „SOOVITATAV”, „VÕIB” ja „VALIKULINE” tõlgendada niiviisi, nagu kirjeldatud dokumendis RFC 2119 ([1]).

PUNKT 1. XAdES-BES/EPES

Allkiri vastab W3C XMLi allkirja spetsifikaadile ([2]).

Allkiri PEAB olema vähemalt XAdES-BESi (või -EPESi) allkirja vormis, nagu kirjeldatud ETSI TS 101 903 XAdESi spetsifikaadis, ([3]) ning vastab kõigile järgmistele täiendavatele spetsifikaatidele.

Meetod ds:CanonicalizationMethod, mis määrab kindlaks kanoniseerimise algoritmi, mida rakendatakse SignedInfo-elemendile enne allkirja arvutuste teostamist, on ainult üks järgmistest algoritmidest:

kanooniline XML 1.0 (ei sisalda kommentaare):	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
kanooniline XML 1.1 (ei sisalda kommentaare):	http://www.w3.org/2006/12/xml-c14n11
eksklusiivne XML, kanoniseerimine 1.0 (ei sisalda kommentaare):	http://www.w3.org/2001/10/xml-exc-c14n#

Teisi algoritme ega ülal loetletud algoritmide „Kommentaaridega” versioone EI PEAKS allkirja loomiseks kasutatama, kuid allkirjade verifitseerimisel PEAKS neid toetatama, et tagada koostalitlusvõime varem kasutatud algoritmide osas.

MD5 (RFC 1321)-d EI TOHI kasutada räsialgoritmina. Allkirja andjatel soovitatakse tutvuda kohaldatavate riigisiseste seadustega ning juhiste saamiseks dokumendiga ETSI TS 102 176 ([4]) ning täiendavate soovituste saamiseks elektronallkirjade puhul lubatavate algoritmide ja parameetrite kohta raportiga ECRYPT2 D.SPA.x ([5]).

Transformidest võib kasutada ainult järgmisi.

Kanoniseerimise transformid: vt ülal esitatud seonduvaid spetsifikaate

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

Filtreerimine

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): ühilduvuse jaoks ning vastavuseks XMLDSig'iga.

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): järglasena XPath'ile töökindluse jaoks.

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

XSLT (laaditabel) **transform**.

Element ds:KeyInfo PEAB sisaldama allkirjastaja X.509 v3 digitaalset sertifikaati (st selle väärtust ja mitte ainult viidet sellele).

„SigningCertificate'i” allkirjastatud allkirjavara PEAB sisaldama räsiväärtust (CertDigest) ja allkirjastaja sertifikaadi seerianumbrit (IssuerSerial), mis on talletatud elemendis ds:KeyInfo, ning valikulist URI väljal „SigningCertificate” EI TOHI kasutada.

SigningTime'i allkirjastatud allkirjavara on olemas ja sisaldab UTC-d, mis on väljendatud kujul xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

Element DataObjectFormat PEAB olema olemas ja sisaldama MimeType'i alamelementi.

Juhul kui liikmesriikide kasutatavad allkirjad põhinevad kvalifitseeritud sertifikaadil, on allkirjas sisalduvad PKI-objektid (sertifikaadi ahelad, kehtivusinfo, ajatemplid) verifitseeritavad vastavalt otsusele 2009/767/EÜ, kasutades selle liikmesriigi usaldusnimekirja, kes teostab järelevalvet selle sertifitseerimisteenuse osutaja üle või akrediteerib seda sertifitseerimisteenuse osutajat, kes allkirjastaja sertifikaadi väljastas.

Tabelis 1 on esitatud kokkuvõtlikult spetsifikaadid, millele XAdES-BES/EPES-allkiri peab vastama, et saaja-liikmesriigi süsteemid seda tehniliselt toetaksid.

([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]) Viimane versioon on D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), 30. märts 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabel 1

XAdES - BES (EPES)		**Ühtsed miinimumnõuded**
(ETSI TS 103 903 rakendatakse järgmiste profiilielementidega)		
K = kohustuslik; V = valikuline; S = soovituslik; E = ei ole kasutusel		
ds: Signature ID	K	
ds: SignedInfo	K	
ds: CanonicalizationMethod	K	*Allkirjade verifitseerimisel PEAB süsteem toetama kõiki järgmisi algoritme, nende loomisel PEAKS süsteem aga olema piiratud ühega neist:* *- eksklusiivne XML kanoniseerimine 1.0: http://www.w3.org/TR/xml-exc-c14n/* *- kanooniline XML 1.0: http://www.w3.org/TR/2001/REC-XML-c14n-20010315* *- kanooniline XML 1.1: http://www.w3.org/2006/12/xml-c14n11* *Teisi meetodeid ega ülal loetletud meetodite "#WithComments" versioone EI PEAKS süsteem kasutama.*
ds: SignatureMethod	K	***Algoritmid: vt kohaldatavaid riiklikke seadusi ning juhiste saamiseks dokumenti ETSI TS 102 176 ning täiendavate soovituste saamiseks raportit ECRYPT2 D.SPA.7.***
ds: Reference URI	K	Üks referents iga allkirjastatava andmeobjekti kohta (URI-d võivad osutada ka välistele objektidele) + referents elemendile SignedProperties.
ds: Transforms	V	*Verifitseerimisrakendused PEAVAD toetama kõiki järgmisi transforme, samas kui allkirja loomise rakendus PEAKS piirama nende transformide kasutamist vaid järgmistele:* *- kanoniseerimise transformid: vt ülal* *- Base64 kodeerimine* *- XPath ja XPath Filter 2.0* *- ümbrikusse pandud allkirja transform* *- XSLT transformid*
ds: DigestMethod	K	***Algoritmid: vt kohaldatavaid riigisiseseid seadusi ning juhiste saamiseks dokumenti ETSI TS 102 176 ning täiendavate soovituste saamiseks raportit ECRYPT2 D.SPA.7.***
ds: DigestValue	K	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	K	
ds: KeyInfo	K	PEAB sisaldama X509 sertifikaate (SigningCertificate'i allkirjastatud vara PEAB sisaldama selle allkirjastaja sertifikaadi räsiväärtust) Verifitseerimisprotsessi lihtsustamiseks on SOOVITATAV esitada vihjena allkirjastaja sertifikaadi sertifitseerimisahel (sel juhul PEAVAD olema esitatud X.509 sertifikaadid).
ds: Object		
QualifyingProperties	K	
SignedProperties	K	M
SignedSignatureProperties	K	M
SigningTime	K	UTC (xsd: dateTime).
SigningCertificate	K	PEAB sisaldama ds:KeyInfo's talletatud allkirjastaja sertifikaadi räsiväärtust ning valikuline URI jäetakse välja (rakendused VÕIVAD otsida/leida allkirjastaja sertifikaati ds:KeyInfo's räsiekvivalentsi alusel).
SignaturePolicyIdentifier	V	Ainult EPES-vormi puhul (ning kõrgemate vormide puhul, mis on üles ehitatud EPES-vormist)
Signature ProductionPlace	V	
SignerRole	V	
/SignedSignatureProperties		
SignedDataObjectProperties	V	
DataObjectFormat	K	Kui on kasutatud seda välja, TULEB rakendustes tagada, et andmeobjektid oleksid kasutajale vastavalt näidatud. Kui seda kasutatakse, PEAB kasutama MimeType'i alamelementi.
CommitmentTypeIndication	V	
AllDataObjectsTimeStamp	V	
IndividualDataObjectTimeStamp	V	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	V	
UnsignedSignatureProperties		
CounterSignature	V	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Allkirja topoloogia. Allkirjastatud originaalfailide ja allkirjade pakkimine		
SignatureEnveloped		Kõik PEAVAD olema toetatud
SignatureEnveloping		
SignatureDetached		

PUNKT 2. CAdES-BES/EPES

Allkiri vastab Cryptographic Message Syntaxi (CMS) allkirja spetsifikaadile ([1]).

Allkiri kasutab CAdES-BESi (või -EPESi) allkirja atribuute, nagu kirjeldatud ETSI TS 101 733 CAdESi spetsifikaadis, ([2]) ning vastab täiendavatele spetsifikaatidele, nagu esitatud allpool tabelis 2.

Kõik CAdESi atribuudid, mis sisalduvad arhiivi ajatempli räsikalkulatsioonis (ETSI TS 101 733 V1.8.1 lisa K), PEAVAD olema DER-krüpteeringus ja mis tahes muud atribuudid võivad olla BERis, et lihtsustada CAdESi ühekäigulist töötlemist.

MD5 (RFC 1321) EI TOHI kasutada räsialgoritmina. Allkirja andjatel soovitatakse tutvuda kohaldatavate riigisiseste seadustega ning juhiste saamiseks dokumendiga ETSI TS 102 176 ([3]) ning täiendavate soovituste saamiseks elektronallkirjade puhul lubatavate algoritmide ja parameetrite kohta raportiga ECRYPT2 D.SPA.x ([4]).

Allkirjastatud atribuudid PEAVAD sisaldama viidet allkirjastaja X.509 v3 digitaalsele sertifikaadile (RFC 5035) ning väli „*SignedData.certificates*" PEAB sisaldama selle väärtust;

Allkirjastatud atribuut SigningTime PEAB olema olemas ja PEAB sisaldama UTCd, mis on väljendatud nagu lehel http://tools.ietf.org/html/rfc5652#section-11.3.

Allkirjastatud atribuut ContentType PEAB olema olemas ning sisaldab id-andmeid (http://tools.ietf.org/html/rfc5652#section-4), kus andmete sisu tüüp on mõeldud osutamaks suvalistele oktett-stringidele, nagu UTF-8 tekst või ZIP-konteiner koos MimeType'i alamelemendiga.

Juhul kui liikmesriikide kasutatavad allkirjad põhinevad kvalifitseeritud sertifikaadil, on allkirjas sisalduvad PKI-objektid (sertifikaadi ahelad, kehtivusinfo, ajatemplid) verifitseeritavad vastavalt otsusele 2009/767/EÜ, kasutades selle liikmesriigi usaldusnimekirja, kes teostab järelevalvet selle sertifitseerimisteenuse osutaja üle või akrediteerib seda sertifitseerimisteenuse osutajat, kes allkirjastaja sertifikaadi väljastas.

([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]) Viimane versioon on D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), 30. märts 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabel 2

CAdES - BES (EPES)		**Ühtsed miinimumnõuded**
(ETSI TS 101 733 rakendatakse järgmiste profiilielementidega)		
ASN.1		
`ContentInfo ::= SEQUENCE {`		
`contentType ContentType, -- id-signedData`		
`content [0] EXPLICIT ANY DEFINED BY contentType }`		
K = kohustuslik; V = valikuline; S = soovituslik; E = ei ole kasutusel		
`SignedData ::= SEQUENCE {`		
`version CMSVersion,`		
`digestAlgorithms DigestAlgorithmIdentifiers,`	K	Algoritmid: vt kohaldatavaid riigisiseseid seadusi ning juhiste saamiseks dokumenti ETSI TS 102 176 ning täiendavate soovituste saamiseks raportit ECRYPT2 D.SPA.7.
`encapContentInfo SEQUENCE {`		
`eContentType ContentType,`	K	id-Data
`eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },`	K/E	Allkirjastatud atribuut ContentType on olemas ja sisaldab id-andmeid (http://tools.ietf.org/html/rfc5652#section-4), kus andmete sisu tüüp on mõeldud osutamaks suvalistele oktett-stringidele, nagu UTF-8 text või ZIP-konteiner koos MimeType'i alamelemendiga
`-- External Data (välised andmed – kui allkiri on eraldatud)*`		Kui eraldatud allkirja ei ole muidu olemas. * Välised andmed tähendavad andmeid, mis on kaitstud eraldatud allkirjaga, mis ei sisaldu CAdES-allkirja eContent`is. On soovitatav lisada allkirjastatud välised andmed koos allkirjaga ZIP-faili.
`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	K	PEAB sisaldama allkirjastajalt X509 sertifikaati. Sertifikaatide lisamine kogu sertifitseerimisahelast kuni usaldusankruni on SOOVITATAV.
`crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,`	V	
`signerInfos SET OF`	K	Vähemalt üks signerInfo
`SEQUENCE { -- SignerInfo`		
`version CMSVersion,`		
`sid SignerIdentifier,`	V	(Kaitsmata väärtus)
`digestAlgorithm DigestAlgorithmIdentifier,`	K	Algoritmid: vt kohaldatavaid riigisiseseid seadusi ning juhiste saamiseks dokumenti ETSI TS 102 176 ning täiendavate soovituste saamiseks raportit ECRYPT2 D.SPA.7.
`signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF`		
`SEQUENCE { -- Attribute`	K	
`attrType OBJECT IDENTIFIER,`	K/V	PEAB: id-contentType (id-andmetega) id-messageDigest id-aa-ets-signingCertificateV2 või id-aa-signingCertificate PEAB: signingTime VALIKULINE: id-aa-ets-sigPolicyId Muud valikulised atribuudid, nagu määratletud dokumendis ETSI TS 101 733.
`attrValues SET OF AttributeValue } VALIKULINE,`		
`signatureAlgorithm SignatureAlgorithmIdentifier,`		Algoritmid: vt kohaldatavaid riigisiseseid seadusi ning juhiste saamiseks dokumenti ETSI TS 102 176 ning täiendavate soovituste saamiseks raportit ECRYPT2 D.SPA.7.
`signature OCTET STRING, -- SignatureValue`		
`unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF`	V	
`SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }`	V	

PUNKT 3. PAdES-PART 3 (BES/EPES)

Allkirjas PEAB olema kasutatud PAdES-BESi (või -EPESi) allkirja laiendit, nagu kirjeldatud ETSI TS 102 778 PAdES-Part3 spetsifikaadis, ([1]) ning see vastab järgmistele täiendavatele spetsifikaatidele.

MD5 (RFC 1321) EI TOHI kasutada räsialgoritmina. Allkirja andjatel soovitatakse tutvuda kohaldatavate riigisiseste seadustega ning juhiste saamiseks dokumendiga ETSI TS 102 176 ([2]) ning täiendavate soovituste saamiseks elektronallkirjade puhul lubatavate algoritmide ja parameetrite kohta raportiga ECRYPT2 D.SPA.x ([3]).

Allkirjastatud atribuudid PEAVAD sisaldama viidet allkirjastaja X.509 v3 digitaalsele sertifikaadile (RFC 5035) ning väli „*SignedData.certificates*" PEAB sisaldama selle väärtust.

([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]) Viimane versioon on D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), 30. märts 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Allkirjastamise aega näitab allkirja sõnastikus kirje **M** väärtus.

Juhul kui liikmesriikide kasutatavad allkirjad põhinevad kvalifitseeritud sertifikaadil, on allkirjas sisalduvad PKI-objektid (sertifikaadi ahelad, kehtivusinfo, ajatemplid) verifitseeritavad vastavalt otsusele 2009/767/EÜ, kasutades selle liikmesriigi usaldusnimekirja, kes teostab järelevalvet selle sertifitseerimisteenuse osutaja üle või akrediteerib seda sertifitseerimisteenuse osutajat, kes allkirjastaja sertifikaadi väljastas.