SPRENDIMAI

KOMISIJOS SPRENDIMAS

2011 m. vasario 25 d.

kuriuo nustatomi būtinieji dokumentų, kompetentingų institucijų pasirašomų elektroniniu būdu pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje, tarptautinio tvarkymo reikalavimai

(pranešta dokumentu Nr. C(2011) 1081)

(Tekstas svarbus EEE)

(2011/130/ES)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2006 m. gruodžio 12 d. Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje [1], ypač į jos 8 straipsnio 3 dalį,

kadangi:

(1) Paslaugų teikėjai, kurių paslaugoms taikoma Direktyva 2006/123/EB, privalo turėti galimybę per kontaktinius centrus arba elektroninėmis priemonėmis atlikti procedūras ir formalumus, reikalingus norint užsiimti savo veikla ir ją vykdyti. Laikantis Direktyvos 2006/123/EB 5 straipsnio 3 dalyje nustatytų ribų, vis tiek galimi atvejai, kai paslaugų teikėjai, atlikdami tokias procedūras ir formalumus, turi pateikti dokumentų originalus, patvirtintas kopijas arba patvirtintus vertimus. Tais atvejais paslaugų teikėjams gali prireikti pateikti kompetentingų institucijų elektroniniu būdu pasirašytus dokumentus.

(2) Sąlygos tarptautiniu mastu naudoti saugius elektroninius parašus su kvalifikuotu sertifikatu pagerinamos 2009 m. spalio 16 d. Komisijos sprendimu 2009/767/EB, kuriuo pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje [2] nustatomos priemonės procedūroms, atliekamoms naudojantis elektroninėmis priemonėmis ir kontaktinių centrų paslaugomis, palengvinti; šiuo sprendimu, *inter alia*, valstybės narės įpareigojamos atlikti rizikos vertinimus prieš tai, kai jos pareikalauja, kad paslaugų teikėjai naudotų tokius elektroninius parašus, ir nustatomos taisyklės, kaip valstybės narės turėtų priimti saugius elektroninius parašus, grindžiamus kvalifikuotais sertifikatais ir sukurtus naudojant saugią parašų kūrimo priemonę arba jos nenaudojant. Tačiau, Sprendime 2009/767/EB nesprendžiamas klausimas dėl elektroninių parašų formato kompetentingų institucijų išduotuose dokumentuose, kuriuos, atlikdami atitinkamas procedūras ir formalumus, turi pateikti paslaugų teikėjai.

(3) Kadangi valstybių narių kompetentingos institucijos savo dokumentams elektroniniu būdu pasirašyti dabar naudoja skirtingų formatų saugius elektroninius parašus, šiuos dokumentus gaunančios ir juos tvarkyti turinčios valstybės narės dėl naudojamų parašų formatų įvairovės gali patirti techninių sunkumų. Kad paslaugų teikėjai galėtų tarpvalstybines procedūras ir formalumus atlikti elektroninėmis priemonėmis, valstybėms narėms, gaunančioms kitų valstybių narių kompetentingų institucijų elektroniniu būdu pasirašomus dokumentus, turėtų būti sudarytos techninės sąlygos priimti bent jau keleto formatų elektroninius parašus. Apibrėžus tam tikrus saugių elektroninių parašų formatus, kuriems priimti gaunančioje valstybėje narėje turi būti sudarytos techninės sąlygos, būtų užtikrinta didesnė automatizacija ir padidintas tarpvalstybinis elektroninių procedūrų tarpusavio sąveikumas.

(4) Valstybės narės, kurių kompetentingos institucijos naudoja ne visuotinai priimtus elektroninių parašų formatus, gali būti įgyvendinusios patvirtinimo priemones, leidžiančias patikrinti jų parašus ir tarpvalstybiniu mastu. Todėl, kad dokumentus gaunančios valstybės narės galėtų pasitikėti šiomis patvirtinimo priemonėmis, reikia užtikrinti, kad informacija apie jas būtų lengvai prieinama, nebent reikiama informacija tiesiogiai įtraukta į elektroninius dokumentus, elektroninius parašus arba elektroninių dokumentų laikmenas.

(5) Šis sprendimas neturi poveikio valstybių narių sprendimui, kas yra originalas, patvirtinta kopija ar patvirtintas vertimas. Jo tikslas – tik pagerinti galimybę tikrinti elektroninius parašus, jeigu jie naudojami originaluose, patvirtintose kopijose arba patvirtintuose vertimuose, kuriuos paslaugų teikėjams gali tekti pateikti per kontaktinius centrus.

[1] OL L 376, 2006 12 27, p. 36.
[2] OL L 274, 2009 10 20, p. 36.

(6) Siekiant valstybėms narėms sudaryti sąlygas įgyvendinti reikiamas technines priemones, tikslinga šį sprendimą taikyti nuo 2011 m. rugpjūčio 1 d.

(7) Šiame sprendime numatytos priemonės atitinka Paslaugų direktyvos komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Orientacinis elektroninių parašų formatas

1. Valstybės narės įgyvendina reikiamas technines priemones, leidžiančias joms tvarkyti elektroniniu būdu pasirašytus dokumentus, kuriuos, atlikdami procedūras ir formalumus, per kontaktinius centrus pateikia paslaugų teikėjai, kaip numatyta Direktyvos 2006/123/EB 8 straipsnyje, ir kuriuos BES arba EPES formato saugiu XML, CMS arba PDF elektroniniu parašu, atitinkančiu priede išdėstytas technines specifikacijas, yra pasirašiusios kitų valstybių narių kompetentingos institucijos.

2. Valstybės narės, kurių kompetentingos institucijos 1 dalyje nurodytus dokumentus pasirašo ne šioje dalyje patvirtintų formatų elektroniniais parašais, praneša Komisijai apie esamas patvirtinimo galimybes, kuriomis pasinaudodamos kitos valstybės narės gautus elektroninius parašus gali nemokamai patvirtinti internetu asmenims, kuriems tai nėra gimtoji kalba, suprantamu būdu, nebent reikiama informacija jau įtraukta į dokumentą, elektroninį parašą arba elektroninio dokumento laikmeną. Komisija perduos tą informaciją visoms valstybėms narėms.

2 straipsnis

Taikymas

Šis sprendimas taikomas nuo 2011 m. rugpjūčio 1 d.

3 straipsnis

Adresatai

Šis sprendimas skirtas valstybėms narėms.

Priimta Briuselyje 2011 m. vasario 25 d.

Komisijos vardu
Michel BARNIER
Komisijos narys

PRIEDAS

XML, CMS arba PDF saugaus elektroninio parašo, kurio techninį palaikymą turi užtikrinti gaunančioji valstybė narė, specifikacijos

Šioje dokumento dalyje raktiniai žodžiai „PRIVALO“, „DRAUDŽIAMA“, „PRIVALOMAS“, „TURI“, „NETURI“, „TURĖTŲ“, „NETURĖTŲ“, „REKOMENDUOJAMA“, „GALI“ ir „NEPRIVALOMAS“ turi būti suprantami taip, kaip aprašyta RFC 2119 ([1]).

1 SKIRSNIS – XAdES-BES/EPES:

Parašas atitinka W3C XML parašo specifikacijas ([2]).

Parašas PRIVALO būti bent XAdES-BES (arba -EPES) parašo formato, kaip nustatyta ETSI TS 101 903 XAdES specifikacijose ([3]), ir atitikti visas šias papildomas specifikacijas.

Taikant *ds:CanonicalizationMethod*, kuriuo nustatomas kanonizavimo algoritmas, taikomas SignedInfo elementui prieš atliekant parašo skaičiavimus, identifikuojamas tik vienas iš šių algoritmų:

Canonical XML 1.0 (be komentarų) – http://www.w3.org/TR/2001/REC-xml-c14n-20010315;

Canonical XML 1.1 (be komentarų) – http://www.w3.org/2006/12/xml-c14n11;

Exclusive XML Canonicalization 1.0 (be komentarų) – http://www.w3.org/2001/10/xml-exc-c14n#.

Kiti algoritmai arba minėtų algoritmų versijos su komentarais NETURĖTŲ būti naudojami parašams formuoti, tačiau TURĖTŲ būti palaikomi parašo patikros liekamajam sąveikumui užtikrinti.

MD5 (RFC 1321) DRAUDŽIAMA naudoti kaip maišos algoritmą. Pasirašantieji turi vadovautis taikomais nacionaliniais teisės aktais, o papildomų rekomendacijų apie elektroniniams parašams tinkamus algoritmus ir parametrus ieškoti ETSI TS 102 176 ([4]) ir ECRYPT2 D.SPA.x ataskaitoje ([5]).

Leidžiama naudoti tik šiuo *transformavimo būdus*:

kanonizavimo transformavimas (žr. ankstesnes susijusias specifikacijas);

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

Filtravimas

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116) – skirta suderinamumui ir atitikčiai su XMLDSig;

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2) – kaip XPath pakaitalas dėl funkcinių aspektų.

Įtrauktojo (angl. enveloped) parašo transformavimas – (http://www.w3.org/2000/09/xmldsig#enveloped-signature).

XSLT (*style sheet*) **transformavimas**.

Į elementą *ds:KeyInfo* PRIVALO būti įtrauktas pasirašančiojo X.509 v3 skaitmeninis sertifikatas (t. y. jo vertė, o ne tik nuoroda į jį).

Į pasirašyto parašo savybę „SigningCertificate“ PRIVALO būti įtraukta pasirašančiojo sertifikato maišos vertė (*CertDigest*) ir *IssuerSerial*, saugoma elemente *ds:KeyInfo*, o neprivalomąjį URI lauke „SigningCertificate“ naudoti DRAUDŽIAMA;

Pasirašyto parašo savybė *SigningTime* naudojama ir joje nurodomas UTC laikas, išreikštas formatu *xsd:dateTime* (http://www.w3.org/TR/xmlschema-2/#dateTime).

Elementas *DataObjectFormat* PRIVALO BŪTI ir turėti poelementį *MimeType*.

Jei valstybių narių naudojami parašai paremti kvalifikuotu sertifikatu, į parašus įtraukti PKI objektai (sertifikatų grandinės, atšaukimo duomenys, laiko žymos) patikrinami naudojantis valstybės narės, kuri prižiūri arba akredituoja pasirašančiojo sertifikatą išdavusį CSP, patikimu sąrašu, sudarytu pagal Komisijos sprendimą 2009/767/EB.

1 lentelėje pateikiamos specifikacijos, kurias turi atitikti XAdES-BES/EPES parašas, kad jis galėtų būti techniškai palaikomas gaunančioje valstybėje narėje.

([1]) IETF RFC 2119: „Raktiniai žodžiai, naudojami RFC būtinumo lygiams nurodyti“.
([2]) W3C, XML parašų sintaksė ir apdorojimas (1.1 versija), http://www.w3.org/TR/xmldsig-core1/.
W3C, XML parašų sintaksė ir apdorojimas (antrasis leidimas), http://wwsw.w3.org/TR/xmldsig-core/.
W3C, XML geriausia parašų diegimo patirtis, http://www.w3.org/TR/xmldsig-bestpractices/.
([3]) ETSI TS 101 903 v1.4.1: XML saugūs elektroniniai parašai (XAdES).
([4]) ETSI TS 102 176: Elektroniniai parašai ir infrastruktūros (ESI); Saugių elektroninių parašų algoritmai ir parametrai; 1 dalis. Maišos funkcijos ir asimetriniai algoritmai; 2 dalis. Parašų formavimo įrangos saugaus kanalo protokolai ir algoritmai.
([5]) Naujausia versija yra D.SPA.13 ECRYPT2 Algoritmų ir raktų dydžių metinė ataskaita (2009–2010 m.), išleista 2010 m. kovo 30 d. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

1 lentelė

XAdES - BES (EPES)		**Bendrieji būtiniausi reikalavimai**
(Taikomos ETSI TS 103 903 su toliau nurodytais aprašo elementais)		
M – privalomas; O – neprivalomas; R – rekomenduojamas; N – nenaudojamas		
ds: Signature ID	M	
ds: SignedInfo	M	
ds: CanonicalizationMethod	M	*Visi toliau nurodyti algoritmai TURI būti palaikomi parašui patikrinti, formuojant TURĖTŲ būti apsiribota vienu iš šių:* *- 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* *Kiti metodai arba minėtų metodų versijos "#WithComments" NETURĖTŲ būti naudojami.*
ds: SignatureMethod	M	***Algoritmai*** *– vadovaukitės taikomais nacionaliniais teisės aktais, o rekomendacijų ieškokite ETSI TS 102 176 ir ECRYPT2 D.SPA.7 ataskaitoje*
ds: Reference URI	M	Viena nuoroda į kiekvieną pasirašomą pradinių duomenų objektą (URIs gali nurodyti ir išorinį objektą) + nuoroda į *SignedProperties* elementą
ds: Transforms	O	*Tikrinimo taikomosios programos PRIVALO palaikyti visus toliau nurodytus transformavimo būdus, o parašo formavimo taikomoji programa TURĖTŲ apsiriboti tokiu transformavimu:* *- kanonizavimo transformavimu (žr. pirmiau)* *- Base64 koduote* *- XPath ir XPath filtru 2.0* *- "Enveloped" parašo transformavimu* *- XSLT transformavimu*
ds: DigestMethod	M	***Algoritmai*** *– vadovaukitės taikomais nacionaliniais teisės aktais, o rekomendacijų ieškokite ETSI TS 102 176 ir ECRYPT2 D.SPA.7 ataskaitoje*
ds: DigestValue	M	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	M	
ds: KeyInfo	M	PRIVALO turėti X509 sertifikatą (į pasirašytą savybę *SigningCertificate* PRIVALO būti įtraukta šio pasirašančiojo sertifikato maišos vertė) REKOMENDUOJAMA pateikti pasirašančiojo sertifikato sertifikavimo grandinę, kaip užuominą patvirtinimo procesui palengvinti (šiuo atveju PRIVALU pateikti X.509 sertifikatus).
ds: Object		
QualifyingProperties	M	
SignedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC (xsd: dateTime).
SigningCertificate	M	PRIVALO būti pasirašančiojo sertifikato maišos vertė, laikoma elemente *ds:KeyInfo* , o neprivalomas URI praleidžiamas (taikomosios programos GALI ieškoti ir rasti pasirašančiojo sertifikatą elemente *ds:KeyInfo* remdamosi maišos atitikimu).
SignaturePolicyIdentifier	O	tik EPES formai (ir aukštesnėms formoms, sudarytoms iš EPES formos)
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	M	Kai šis laukas naudojamas, taikomosios programos PRIVALO užtikrinti, kad duomenų objektai vartotojui būtų rodomi atitinkamai. Kai naudojama, PRIVALO būti naudojamas *MimeType* pavaldusis elementas.
CommitmentTypeIndication	O	
AllDataObjectsTimeStamp	O	
IndividualDataObjectTimeStamp	O	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	O	
UnsignedSignatureProperties		
CounterSignature	O	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Parašo topologija – pasirašytų pradinių failų ir parašų archyvavimas		
SignatureEnveloped		Visi PRIVALO būti palaikomi
SignatureEnveloping		
SignatureDetached		

2 SKIRSNIS – CAdES-BES/EPES:

Parašas atitinka kriptografinio pranešimo sintaksės (CMS) parašo specifikacijas ([1]).

Paraše naudojami CAdES-BES (arba -EPES) parašo atributai, nurodyti ETSI TS 101 733 CAdES specifikacijose ([2]), ir jis atitinka 2 lentelėje nurodytas papildomas specifikacijas.

Visi CAdES atributai, kurie yra įtraukti į archyvavimo laiko žymos maišos skaičiavimą (ETSI TS 101 733 V1.8.1 K priedas) PRIVALO būti DER koduotės, o visi kiti gali būti BER koduotės, kad supaprastėtų CAdES apdorojimas viena operacija.

MD5 (RFC 1321) DRAUDŽIAMA naudoti kaip maišos algoritmą. Pasirašantieji turi vadovautis taikomais nacionaliniais teisės aktais, o papildomų rekomendacijų apie elektroniniams parašams tinkamus algoritmus ir parametrus reikia ieškoti ETSI TS 102 176 ([3]) ir ECRYPT2 D.SPA.x ataskaitoje ([4]).

Į pasirašytus atributus PRIVALO būti įtraukta nuoroda į pasirašančiojo skaitmeninį sertifikatą X.509 v3 (RFC 5035), o lauke *SignedData.certificates* PRIVALO būti nurodyta jo vertė.

PRIVALO būti pasirašytas *SigningTime* atributas ir jame PRIVALO būti UTC laikas, išreikštas formatu, nurodytu http://tools.ietf.org/html/rfc5652#section-11.3.

PRIVALO būti pasirašytas *ContentType* atributas, kuriame yra tapatybės duomenys (*id-data*) (http://tools.ietf.org/html/rfc5652#section-4), kurių turinio tipas skirtas nurodyti pasirenkamas aštuonženkles sekas, pvz., UTF-8 tekstas arba ZIP archyvas su *MimeType* poelemenčiu.

Jei valstybių narių naudojami parašai paremti kvalifikuotu sertifikatu, į parašus įtraukti PKI objektai (sertifikatų grandinės, atšaukimo duomenys, laiko žymos) patikrinami naudojantis valstybės narės, kuri prižiūri arba akredituoja pasirašančiojo sertifikatą išdavusį CSP, patikimu sąrašu, sudarytu pagal Komisijos sprendimą 2009/767/EB.

([1]) IETF, RFC 5652, Kriptografinio pranešimo sintaksė (CMS), http://tools.ietf.org/html/rfc5652.
IETF, RFC 5035, Padidinto saugumo paslaugos (ESS). Naujinys: papildymas CertID algoritmo judrumu, http://tools.ietf.org/html/rfc5035.
IETF, RFC 3161, Interneto X.509 atvirojo rakto infrastruktūros laiko žymos protokolas (TSP), http://tools.ietf.org/html/rfc3161.

([2]) ETSI TS 101 733 v.1.8.1: CMS saugūs elektroniniai parašai (CAdES).

([3]) ETSI TS 102 176: Elektroniniai parašai ir infrastruktūros (ESI); Saugių elektroninių parašų algoritmai ir parametrai; 1 dalis: Maišos funkcijos ir asimetriniai algoritmai; 2 dalis: Parašų formavimo įrangos Saugaus kanalo protokolai ir algoritmai.

([4]) Naujausia versija yra D.SPA.13 ECRYPT2 Algoritmų ir raktų dydžių metinė ataskaita (2009–2010 m.), išleista 2010 m. kovo 30 d. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

2 lentelė

CAdES - BES (EPES)		**Bendrieji būtiniausi reikalavimai**
(Taikomos ETSI TS 103 903 su toliau nurodytais aprašo elementais)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
M – privalomas; O – neprivalomas; R – rekomenduojamas; N – nenaudojamas		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	**M**	**Algoritmai – vadovaukitės taikomais nacionaliniais teisės aktais, o rekomendacijų ieškokite ETSI TS 102 176 ir ECRYPT2 D.SPA.7 ataskaitoje**
encapContentInfo SEQUENCE {		
eContentType ContentType,	**M**	**id-Data**
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	**M/N**	**Yra pasirašytas *ContentType* atributas, kuriame yra tapatybės duomenys (*id-data*) (http://tools.ietf.org/html/rfc5652#section-4), kurių turinio tipas skirtas nurodyti pasirenkamas aštuonženkles sekas, pvz., UTF-8 tekstas arba ZIP archyvas su *MimeType* poelemenčiu**
-- External Data (if signature detached)*		**jei atskirto parašo kitaip nėra. * išoriniai duomenys - tai duomenys, apsaugoti atskirtu parašu, kuris neįtrauktas į CAdES parašo *eContent* . Rekomenduojama pasirašytus išorinius duomenis kartu su parašu įtraukti į ZIP failą.**
certificates [0] IMPLICIT CertificateSet OPTIONAL,	**M**	**PRIVALO turėti pasirašančiojo X509 sertifikatą. REKOMENDUOJAMA įtraukti visos sertifikavimo grandinės sertifikatus iki pat saugumą užtikrinančios priemonės.**
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	**O**	
signerInfos SET OF	**M**	**Bent vienas *signerInfo***
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	**O**	**(Neapsaugota vertė)**
digestAlgorithm DigestAlgorithmIdentifier,	**M**	**Algoritmai – vadovaukitės taikomais nacionaliniais teisės aktais, o rekomendacijų ieškokite ETSI TS 102 176 ir ECRYPT2 D.SPA.7 ataskaitoje**
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	**M**	
attrType OBJECT IDENTIFIER,	**M/O**	**PRIVALOMA id-contentType (su tapatybės duomenimis) id-messageDigest id-aa-ets-signingCertificateV2 arba id-aa-signingCertificate PRIVALOMA: signingTime NEPRIVALOMA id-aa-ets-sigPolicyId Kiti neprivalomi atributai, nustatyti ETSI TS 101 733.**
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmai – vadovaukitės taikomais nacionaliniais teisės aktais, o rekomendacijų ieškokite ETSI TS 102 176 ir ECRYPT2 D.SPA.7 ataskaitoje**
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	**O**	

SEQUENCE {
attrType OBJECT IDENTIFIER,
attrValues SET OF
AttributeValue
} OPTIONAL
}
}
	O	

3 SKIRSNIS – PAdES-PART 3 (BES/EPES):

Paraše PRIVALO būti naudojamas PAdES-BES (arba -EPES) parašo plėtinys, nurodytas ETSI TS 102 778 PAdES-Part3 specifikacijose ([1]), ir jis turi atitikti šias papildomas specifikacijas.

MD5 (RFC 1321) DRAUDŽIAMA naudoti kaip maišos algoritmą. Pasirašantieji turi vadovautis taikomais nacionaliniais teisės aktais, o papildomų rekomendacijų apie elektroniniams parašams tinkamus algoritmus ir parametrus reikia ieškoti ETSI TS 102 176 ([2]) ir ECRYPT2 D.SPA.x ataskaitoje ([3]).

Į pasirašytus atributus PRIVALO būti įtraukta nuoroda į pasirašančiojo skaitmeninį sertifikatą X.509 v3 (RFC 5035), o lauke *SignedData.certificates* PRIVALO būti nurodyta jo vertė.

([1]) ETSI TS 102 778–3 v1.2.1: PDF saugūs elektroniniai parašai (PAdES), PAdES patobulinti – PAdES-Basic elektroniniai parašai ir PAdES-Explicit politikos elektroninių parašų aprašai.

([2]) ETSI TS 102 176: Elektroniniai parašai ir infrastruktūros (ESI); Saugių elektroninių parašų algoritmai ir parametrai; 1 dalis: Maišos funkcijos ir asimetriniai algoritmai; 2 dalis: Parašų formavimo įrangos Saugaus kanalo protokolai ir algoritmai.

([3]) Naujausia versija yra D.SPA.13 ECRYPT2 Algoritmų ir raktų dydžių metinė ataskaita (2009–2010 m.), išleista 2010 m. kovo 30 d. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Pasirašymo data nurodoma **M** įrašo parašo žodyne verte.

Jei valstybių narių naudojami parašai paremti kvalifikuotu sertifikatu, į parašus įtraukti PKI objektai (sertifikatų grandinės, atšaukimo duomenys, laiko žymos) patikrinami naudojantis valstybės narės, kuri prižiūri arba akredituoja pasirašančiojo sertifikatą išdavusį CSP, patikimu sąrašu, sudarytu pagal Sprendimą 2009/767/EB.