ÁKVÖRÐUN FRAMKVÆMDASTJÓRNARINNAR **2015/EES/74/80**

frá 25. febrúar 2011

um að setja lágmarkskröfur um vinnslu skjala yfir landamæri sem undirrituð eru rafrænt af lögbærum yfirvöldum samkvæmt tilskipun Evrópuþingsins og ráðsins 2006/123/EB um þjónustu á innri markaðnum

(tilkynnt með númeri C(2011) 1081)

(2011/130/ESB) (*)

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af tilskipun Evrópuþingsins og ráðsins 2006/123/EB frá 12. desember 2006 um þjónustu á innri markaðnum ([1]), einkum 3. mgr. 8. gr.,

og að teknu tilliti til eftirfarandi:

1) Falli þjónusta þjónustuveitenda undir gildissvið tilskipunar 2006/123/EB þurfa þeir, fyrir milligöngu upplýsinga- og þjónustumiðstöðva og með rafrænum hætti, að geta lokið við þá málsmeðferð og gengið frá þeim formsatriðum sem eru nauðsynleg til að fá aðgang að þjónustustarfsemi og að stunda hana. Innan þeirra marka, sem sett eru í 3. mgr. 5. gr. tilskipunar 2006/123/EB, geta enn verið tilvik þar sem þjónustuveitendur þurfa að leggja fram frumrit skjala, staðfest endurrit eða löggilta þýðingu til að ljúka slíkri málmeðferð og ganga frá formsatriðum. Í slíkum tilvikum geta þjónustuveitendur þurft að leggja fram skjöl sem undirrituð eru rafrænt af lögbærum yfirvöldum.

2) Notkun yfir landamæri á útfærðum rafrænum undirskriftum, sem byggjast á fullgildu vottorði, hefur verið auðvelduð með ákvörðun framkvæmdastjórnarinnar 2009/767/EB frá 16. október 2009 um ráðstafanir sem greiða fyrir notkun rafrænnar málsmeðferðar með upplýsinga- og þjónustumiðstöðvum samkvæmt tilskipun Evrópuþingsins og ráðsins 2006/123/EB um þjónustu á innri markaðnum ([2]), sem m.a. skyldar aðildarríkin til að framkvæma áhættumat áður en þessara rafrænu undirskrifta er krafist af þjónustuveitendum og setur reglur um að aðildarríkin eigi að samþykkja útfærðar rafrænar undirskriftir, sem byggjast á fullgildum vottorðum og gerðar eru með eða án öruggs undirskriftarbúnaðar. Í ákvörðun 2009/767/EB er þó ekki fjallað um snið rafrænna undirskrifta í skjölum, sem lögbær yfirvöld gefa út, sem þjónustuveitendur þurfa að leggja fram þegar þeir ljúka við viðeigandi málsmeðferð og ganga frá formsatriðum.

3) Þar sem lögbær yfirvöld í aðildarríkjum nota nú útfærðar rafrænar undirskriftir með mismunandi sniði til að undirrita skjöl sín með rafrænum hætti geta viðtökuaðildarríkin, sem þurfa að meðhöndla skjölin, lent í tæknilegum vandræðum þar eð snið undirskriftanna er svo fjölbreytt. Til þess að gera þjónustuveitendum kleift að ljúka við málsmeðferð og ganga frá formsatriðum með rafrænum hætti yfir landamæri er nauðsynlegt að tryggja að aðildarríki geti tæknilega stutt við a.m.k. nokkur snið útfærðra rafrænna undirskrifta þegar þau taka við skjölum sem undirrituð eru rafrænt af lögbærum yfirvöldum annarra aðildarríkja. Fastsetning nokkurra sniða útfærðra rafrænna undirskrifta, sem viðtökuaðildarríkið þarf að geta tæknilega stutt við, myndi efla sjálfvirkni og bæta rekstrarsamhæfi rafrænnar málsmeðferðar yfir landamæri.

4) Aðildarríki, þar sem lögbær yfirvöld þess nota önnur snið rafrænna undirskrifta en þau sem eru almennt studd, kunna að hafa innleitt fullgildingaraðferðir sem gerir kleift að staðfesta undirskriftir þeirra einnig yfir landamæri. Ef sú er raunin, og til þess að viðtökuaðildarríkin geti treyst þessum fullgildingaraðferðum, er nauðsynlegt að koma upplýsingum um þessar aðferðir á framfæri á auðveldan og aðgengilegan hátt nema þessar nauðsynlegu upplýsingar komi beint fram í rafrænu skjölunum, í rafrænu undirskriftunum eða flutningsmiðlum rafrænu skjalanna.

5) Ákvörðun þessi hefur ekki áhrif á niðurstöðu aðildarríkjanna um hvað teljist vera frumrit, staðfest endurrit eða löggilt þýðing. Markmið hennar er takmarkað við staðfestingu rafrænna undirskrifta ef þær eru notaðar í frumritunum, staðfestu endurritunum eða löggiltu þýðingunum, sem þjónustuveitendur gætu þurft að leggja fram fyrir milligöngu upplýsinga- og þjónustumiðstöðva.

(*) Þessi EB-gerð birtist í Stjtíð. ESB L 53, 26.2.2011, bls. 66. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 21/2012 frá 10. febrúar 2012 um breytingu á X. viðauka (Almenn þjónusta), sjá EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 34, 21.6.2012, bls. 32.

([1]) Stjtíð. ESB L 376, 27.12.2006, bls. 36.

([2]) Stjtíð. ESB L 274, 20.10.2009, bls. 36.

6) Til að gera aðildarríkjunum kleift að innleiða nauðsynlegan tæknibúnað er rétt að þessi ákvörðun gildi frá og með 1. ágúst 2011.

7) Ráðstafanirnar, sem kveðið er á um í þessari ákvörðun, eru í samræmi við álit nefndarinnar um þjónustutilskipunina.

SAMÞYKKT ÁKVÖRÐUN ÞESSA:

1. gr.

Viðmiðunarsnið fyrir rafrænar undirskriftir

1. Aðildarríki skulu koma á nauðsynlegum tæknilegum úrræðum sem gera þeim kleift að meðhöndla skjöl, sem eru undirrituð rafrænt, sem þjónustuveitendur leggja fram til að ljúka við málsmeðferð og ganga frá formsatriðum fyrir milligöngu upplýsinga- og þjónustumiðstöðva, í samræmi við 8. gr. tilskipunar 2006/123/EB, og sem eru undirrituð af lögbærum yfirvöldum annarra aðildarríkja með útfærðri rafrænni XML-, CMS- eða PDF-undirskrift á BES- eða EPES-sniði, sem er í samræmi við þær tækniforskriftir sem settar eru fram í viðaukanum.

2. Aðildarríki, þar sem lögbær yfirvöld undirrita skjölin sem um getur í 1. mgr. og nota önnur snið rafrænna undirskrifta en þau sem um getur í þeirri málsgrein, skulu tilkynna framkvæmdastjórninni um núverandi möguleika á fullgildingu sem gera öðrum aðildarríkjum kleift að fullgilda þær rafrænu undirskriftir, sem þau taka á móti, á Netinu, án endurgjalds og þannig að það sé skiljanlegt þeim sem hafa annað móðurmál, nema að tilskildar upplýsingar séu þegar innifaldar í skjalinu, í rafrænu undirskiftinni eða í flutningsmiðli rafræna skjalsins. Framkvæmdastjórnin mun gera þessar upplýsingar aðgengilegar öllum aðildarríkjunum.

2. gr.

Gildistími

Ákvörðun þessi gildir frá 1. ágúst 2011.

3. gr.

Viðtakendur

Ákvörðun þessari er beint til aðildarríkjanna.

Gjört í Brussel 25. febrúar 2011.

Fyrir hönd framkvæmdastjórnarinnar,

Michel BARNIER

framkvæmdastjóri.

VIÐAUKI

Forskriftir fyrir útfærðar rafrænar XML-, CMS- eða PDF-undirskriftir sem eiga að vera tæknilega studdar af viðtökuaðildarríkinu

Í eftirfarandi hluta skjalsins skulu eftirfarandi lykilorð túlkuð eins og lýst er í RFC 2119 ([3]): „VERÐUR“ (MUST), „MÁ EKKI“ (MUST NOT), „SKYLDUBUNDIÐ“ (REQUIRED), „SKAL“ (SHALL), „SKAL EKKI“ (SHALL NOT), „ÆTTI“ (SHOULD), „ÆTTI EKKI“ (SHOULD NOT), „MÆLT MEÐ“ (RECOMMENDED), „MÁ“ (MAY) og „VALKVÆTT“ (OPTIONAL).

1. ÞÁTTUR — XAdES-BES/EPES

Undirskriftin er í samræmi við W3C-forskriftir fyrir XML-undirskriftir ([4])

Snið undirskriftarinnar VERÐUR að vera a.m.k. XAdES-BES (eða -EPES) í samræmi við XAdES-forskriftirnar í tækniforskriftum Fjarskiptastaðlastofnunar Evrópu (ETSI TS) 101 903 ([5]) og í samræmi við allar eftirfarandi viðbótarforskriftir:

Aðferðin *„ds:CanonicalizationMethod“*, sem tilgreinir það smættunaralgrím sem beitt er á „SignedInfo“-stakið áður en framkvæmdir eru undirskriftarútreikningar, auðkennir aðeins eitt af eftirfarandi algrímum:

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

Önnur algrím eða útgáfur af framangreindum algrímum „með athugasemdum“ ÆTTI EKKI að nota til að búa til undirskrift en ÆTTI að styðja vegna áframhaldandi rekstrarsamhæfis við sannprófun undirskriftar.

MD5 (RFC 1321) MÁ EKKI nota sem kennialgrím. Undirskriftaraðilum er vísað á gildandi landslög og að því er varðar viðmiðunarreglur um tækniforskriftir Fjarskiptastaðlastofnunar Evrópu (ETSI TS) 102 176 ([6]) og ECRYPT2 D.SPA.x-skýrsluna ([7]) vegna frekari tilmæla um algrím og breytur sem eiga við um rafrænar undirskriftir.

Notkun á vörpunum takmarkast við þær sem skráðar eru hér á eftir:

Smættarvarpanir: sjá tengdar forskriftir hér að framan,

Base64-kóðun (http://www.w3.org/2000/09/xmldsig#base64),

Síun:

XPath http://www.w3.org/TR/1999/REC-xpath-19991116: með tilliti til samhæfis og samkvæmni við XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): sem tekur við af XPath með tilliti til afkastagetu

Hjúpuð undirritunarvörpun (e. *Enveloped Signature transform)*: (http://www.w3.org/2000/09/xmldsig#enveloped-signature).

XSLT-vörpun (stílasafn).

ds:KeyInfo-stakið VERÐUR að innihalda stafrænt X.509 v3-vottorð undirskriftaraðila (þ.e. gildi þess og ekki aðeins tilvísun í það).

Undirritaði undirskriftareiginleikinn „SigningCertificate“ VERÐUR að innihalda kennigildi (CertDigest) og IssueSerial vottorðs undirskriftaraðilans, sem geymt er á *ds:KeyInfo* og valkvætt URI á „SigningCertificate“-svæðinu MÁ EKKI nota.

Undirritaði „SigningTime“-undirritunareiginleikinn er til staðar og inniheldur alheimstíma, gefið upp sem „xsd:dateTime“ (http://www.w3.org/TR/xmlschema-2/#dateTime).

DataObjectFormat-stakið VERÐUR að vera til staðar og innihalda MimeType-undirstakið.

Ef undirritanir, sem aðildarríkin nota, byggjast á fullgildu vottorði þá eru þeir hlutir dreifilyklaskipulags (e. *PKI objects*) (vottorðakeðjur, gögn vegna afturköllunar, tímastimplar) sem eru hluti af undirskriftunum sannprófanlegir með því að nota áreiðanlegan lista þess aðildarríkis sem hefur eftirlit með eða veitir faggildingu til þess vottunaraðila sem gaf út vottorð undirritunaraðila, í samræmi við ákvörðun framkvæmdastjórnarinnar 2009/767/EB.

Í töflu 1 er samantekt yfir þær forskriftir sem XAdES-BES/EPES-undirskrift þarf að uppfylla til að hún sé tæknilega studd af viðtökuaðildarríkinu.

([3]) IETF RFC 2119: „Key words for use in RFCs to indicate Requirements Levels“.

([4]) 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/

([5]) ETSI TS 101 903 v1.4.1: XML Advanced Electronic Signatures (XAdES).

([6]) ETSI TS 102 176: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; 1. hluti: Hash functions and asymmetric algorithms; 2. hluti: „Secure channel protocols and algorithms for signature creation devices“.

([7]) Nýjasta útgáfan er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), frá 30. mars 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tafla 1

XAdES – BES (EPES)		**Sameiginlegar lágmarkskröfur**
(ETSI TS 103 903 á við um eftirfarandi þversniðsstök)		
M=mandatory (skyldubundið); O=optional (valkvætt); R=recommended (mælt með); N=not used (ekki notað)		
ds: Signature ID	M	
ds: SignedInfo	M	
ds: CanonicalizationMethod	M	Öll eftirfarandi algrím VERÐA að styðja sannprófun undirskriftar, myndun ÆTTI að takmarkast við eitt af eftirfarandi: *- Exclusive XML canonicalization 1.0: http://www.w3org/TR/xml-exc-c14n/* *- Canonical XML 1.0: http://www.w3org/TR/2001/REC-XML-c14n-20010315* *- Canonical XML 1.1: http:/www.w3org/2006/12/xml-c14n11* *Aðrar aðferðir eða "#WithComments" útgáfur af framangreindum aðferðum ÆTTI EKKI að nota.*
ds: SignatureMethod	M	***Algrím**: vísar til viðeigandi landslaga og sem viðmiðunarreglur til ETSI TS 102 176 og skýrslunnar ECRYPT2 D.SPA.7 varðandi frekari tilmæli.*
ds: Reference URI	M	Ein tilvísun til sérhvers upprunalegs gagnahlutar sem á að undirrita (URI geta einnig vísað til ytri hluta), + vísun til staksins SignedProperties
ds: Transforms	O	*Sannprófunarforrit VERÐA að styðja eftirfarandi varpanir en nýting til myndunar undirskriftar ÆTTI að takmarka notkun þessara varpana við eftirfarandi:* *Smættarvarpanir: sjá framar* *- Base64 encoding* *- XPath and XPath Filter 2.0* *- Enveloped signature transform* *- XSLT transforms*
ds: DigestMethod	M	***Algrím**: vísar til viðeigandi landslaga og sem viðmiðunarreglur til ETSI TS 102 176 og skýrslunnar ECRYPT2 D.SPA.7 varðandi frekari tilmæli.*
ds: DigestValue	M	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	M	
ds: KeyInfo	M	Verður að hafa X509-vottorð (undirskriftareiginleikinn „SigningCertificate" VERÐUR að innihalda kennigildi vottorðs undirskriftaraðilans) Mælt er með því að vottunarskilríkjakeðja undirskriftaraðila verði látin í té sem vísbending til að greiða fyrir vottunarferlinu (láta VERÐUR X.509-vottorð í té í þessu tilviki).
ds: Object		
QualifyingProperties	M	
SingedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC (xsd: dateTime)
SigningCertificate	M	VERÐUR að innihalda kennigildi vottorðs undirskriftaraðilans sem er geymt á ds: KeyInfo og valkvæðu URI er sleppt (forrit GÆTI leitað að/fundið vottorð undirskriftaraðila á ds: KeyInfo á grundvelli tætijafngildis).
SignaturePolicyIdentifier	O	aðeins fyrir EPES-snið (og fyrir efri snið byggð á EPES-sniði)
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	M	Þegar þessi reitur er notaður SKULU forrit tryggja að gagnahlutir séu sýndir notanda samkvæmt því. Þegar það er notað VERÐUR að nota MimeType undirstak.
CommitmentTypeIndication	O	
AllDataObjectsTimeStamp	O	
IndividualDataObjectTime/Stamp	O	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	O	
UnsignedSignatureProperties		
CounterSignature	O	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Signature topology – Pökkun undirskrifaðra skjala og undirskriftir		
SignatureEnveloped		Styðja VERÐUR allt
SignatureEnveloping		
SignatureDetached		

2. ÞÁTTUR — CAdES-BES/EPES

Undirskriftin er í samræmi við forskriftirnar fyrir undirskrift með málskipan dulkóðaðra skeyta (CMS-undirskrift) ([8]).

Undirskriftin notar CAdES-BES (eða -EPES) eigind undirskriftar sem tilgreind er í CAdES-forskriftunum í tæknilegum forskriftum Fjarskiptastaðlastofnunar Evrópu (ETSI TS) 101 733 ([9]), og fylgir viðbótarforskriftunum eins og vísað er til í töflu 2 hér á eftir.

Sérhver eigind CAdES, sem eru til staðar í tætiútreikningi tímastimplunar í skjalasafninu (viðauki K í tækniforskriftum Fjarskiptastaðlastofnunar Evrópu 101 733 V1.8.1) VERÐUR að vera kóðuð með DER-kóðunarreglum og mega aðrar vera með BER-kóðunarreglum til að einfalda CAdES-vinnslu í einu skrefi (e. *one-pass processing*).

MD5 (RFC 1321) MÁ EKKI nota sem kennialgrím. Undirskriftaraðilum er vísað á gildandi landslög og að því er varðar viðmiðunarreglur um tækniforskriftir Fjarskiptastaðlastofnunar Evrópu (ETSI TS) 102 176 ([10]) og ECRYPT2 D.SPA.x-skýrsluna ([11]) vegna frekari tilmæla um algrím og breytur sem eiga við um rafrænar undirskriftir.

Undirrituð eigind VERÐUR að fela í sér tilvísun í stafrænt X.509 v3-vottorð (RFC 5035) undirskriftaraðila og *SignedData.certificates* svæðið VERÐUR að innihalda gildi þess.

Undirskriftareigindin *„SigningTime“* VERÐUR að vera til staðar og VERÐUR að innihalda UTC, gefið upp eins og í http://tools.ietf.org/html/rfc5652#section-11.3.

Undirritaða eigindin *„ContentType“* VERÐUR að vera til staðar og innihalda gögn um kennimerki (e. *id-data*) (http://tools.ietf.org/htmlertification services/rfc5652#section-4) þar sem efnistag gagnanna (e. *data content type*) er ætlað að vísa til áttundarstrengja af handahófi, eins og UTF-8-texta eða ZIP-geymslueiningar (e. *ZIP container*) með *MimeType*-undirstaki.

Ef undirritanir, sem aðildarríkin nota, byggjast á fullgildu vottorði þá eru þeir hlutir dreifilyklaskipulags (skilríkjakeðjur, gögn vegna afturköllunar, tímastimplar) sem eru hluti af undirskriftunum sannprófanlegir með því að nota áreiðanlega skrá þess aðildarríkis sem hefur eftirlit með eða veitir faggildingu til þess vottunaraðila sem gaf út vottorð undirritunaraðila, í samræmi við ákvörðun framkvæmdastjórnarinnar 2009/767/EB.

([8]) 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.

([9]) ETSI TS 101 733 v.1.8.1: CMS Advanced Electronic Signatures (CAdES).

([10]) ETSI TS 102 176: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; 1. hluti: Hash functions and asymmetric algorithms; 2. hluti: „Secure channel protocols and algorithms for signature creation devices“.

([11]) Nýjasta útgáfan er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), frá 30. mars 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tafla 2

CAdES		**Sameiginlegar lágmarkskröfur**
(ETSI TS 101 733 á við um eftirfarandi þversniðsstök)		
ASN.1		
ContentInfo :: = SEQUENCE {		
contentType ContentType, -- id-signedData		
Content [0] EXPLICIT ANY DEFINED BY content Type }		
M=mandatory (skyldubundið); O=optional (valkvætt); R=recommended (mælt með); N=not used (ekki notað)		
SignedData :: = SEQUENCE {		
Version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	M	Algrím: vísar til viðeigandi landslaga og sem leiðbeiningar til ETSI TS 102 176 og skýrslunnar ENCRYPT2 D.SPA.7 varðandi frekari tilmæli.
encapContentInfo SEQUENCE {		
eContentType ContentType,	M	Id-Data
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- ekki til staðar ef undirskrift er aðskilin },	M/N	Undirritaða eigindin *„ContentType“* VERÐUR að vera til staðar og innihalda gögn um kennimerki (e. *id-data*) (http://tools.ietf.org/html/rfc5652#section-4) þar sem efnistag gagnanna (e. *data content type*) er ætlað að vísa til áttundarstrengja af handahófi, eins og UTF-8-texta eða ZIP-geymslueiningar (e. *ZIP container*) með *MimeType*-undirstaki.
-- Ytri gögn (ef undirskrift er aðskilin)*		ef aðskilin undirskrift er ekki til staðar að öðru leyti. * Ytri gögn merkir gögn sem eru varin með aðskilinni undirskrift sem er ekki undir eContent CAdES-undirskriftar. Mælt er með því að fella undirskrifuð ytri gögn saman við undirskrift í ZIP-skjalinu.
vottorð [0] IMPLICIT CertificateSet OPTIONAL,	M	VERÐUR að hafa X.509-vottorð frá undirskriftaraðila. MÆLT ER MEÐ innfellingu vottorða frá allri undirskriftarkeðjunni allt að áreiðanlegu einindi (e. trust anchor).
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	O	
signerInfos SET OF	M	Minnst eitt signerInfo
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	O	(Ekki varið gildi)
digestAlgorithm DigestAlgorithmIdentifier	M	Algrím: vísar til viðeigandi landslaga og sem leiðbeiningar til ETSI TS 102 176 og skýrslunnar ENCRYPT2 D.SPA.7 varðandi frekari tilmæli.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	M	
attrType OBJECT IDENTIFIER,	M/O	VERÐUR: Id-contentType (with data) Id-messagerDigest Id-aa-ets-signingCertificate V2 or id-aa-signingCertificate VERÐUR: signingTime VALKVÆTT Id-aa-ets-sigPolicyId Aðrar valkvæðar eigindir eins og þær eru skilgreindar í ETSI TS 101 733.
attrValues SET OF AttributeValue }, OPTIONAL		
signatureAlgorithm SignatureAlgorithmIdentifier,		Algrím: vísar til viðeigandi landslaga og sem leiðbeiningar til ETSI TS 102 176 og skýrslunnar ENCRYPT2 D.SPA.7 varðandi frekari tilmæli.
Signature OCTET STRING, -- SignatureValue		

unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF
SEQUENCE {
attrType OBJECT IDENTIFIER,
attrValues SET OF
AttributeValue
} OPTIONAL
}
}
}
	O
	O	

3. ÞÁTTUR — PAdES 3. HLUTI (BES/EPES)

Undirskriftin VERÐUR að nota PAdES-BES- (eða -EPES)-undirskriftarviðauka eins og tilgreint er í 3. hluta í PAdES-forskriftunum í tækniforskriftum Fjarskiptastaðlastofnunar Evrópu (ETSI TS) 102 778 ([12]) og í samræmi við eftifarandi viðbótarforskriftir:

MD5 (RFC 1321) MÁ EKKI nota sem kennialgrím. Undirskriftaraðilum er vísað á gildandi landslög og að því er varðar viðmiðunarreglur um tækniforskriftir Fjarskiptastaðlastofnunar Evrópu (ETSI TS) 102 176 ([13]) og ECRYPT2 D.SPA.x-skýrsluna ([14]) vegna frekari tilmæla um algrím og breytur sem eiga við um rafrænar undirskriftir.

Undirrituð eigind VERÐUR að fela í sér tilvísun í stafrænt X.509 v3-vottorð (RFC 5035) undirskriftaraðila og

([12]) 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.

([13]) ETSI TS 102 176: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; 1. hluti: Hash functions and asymmetric algorithms; 2. hluti: „Secure channel protocols and algorithms for signature creation devices“.

([14]) Nýjasta útgáfan er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), frá 30. mars 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Undirrituð eigind VERÐUR að fela í sér tilvísun í stafrænt X.509 v3-vottorð (RFC 5035) undirskriftaraðila og *SignedData.certificates* svæðið VERÐUR að innihalda gildi þess.

Tími undirritunar er gefinn til kynna með gildinu M í orðasafni undirskriftarinnar.

Ef undirritanir, sem aðildarríkin nota, byggjast á fullgildu vottorði þá eru þeir hlutir dreifilyklaskipulags (skilríkjakeðjur, gögn vegna afturköllunar, tímastimplar) sem eru hluti af undirskriftunum sannprófanlegir með því að nota áreiðanlega skrá þess aðildarríkis sem hefur eftirlit með eða veitir faggildingu til þess vottunaraðila sem gaf út vottorð undirritunaraðila, í samræmi við ákvörðun framkvæmdastjórnarinnar 2009/767/EB.