HATÁROZATOK

A BIZOTTSÁG HATÁROZATA

(2011. február 25.)

az illetékes hatóságok által a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv alapján elektronikusan aláírt dokumentumok országhatáron átnyúló feldolgozására vonatkozó minimumkövetelményekről

(az értesítés a C(2011) 1081. számú dokumentummal történt)

(EGT-vonatkozású szöveg)

(2011/130/EU)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a belső piaci szolgáltatásokról szóló, 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelvre [1] és különösen annak 8. cikke (3) bekezdésére,

mivel:

(1) A 2006/123/EK irányelv hatálya alá tartozó szolgáltatóknak az egyablakos ügyintézési pontokon keresztül elektronikus úton eleget kell tudniuk tenni a tevékenységeikre való jogosultsághoz, illetve azok gyakorlásához kapcsolódó eljárásoknak és alaki követelményeknek. A 2006/123/EK irányelv 5. cikkének (3) bekezdésében megszabott határokon belül továbbra is előfordulhat, hogy a szolgáltatóknak ezen eljárások és alaki követelmények teljesítése során eredeti dokumentumokat, illetve hiteles másolatokat és fordításokat kell benyújtaniuk. Ezekben az esetekben megtörténhet, hogy a szolgáltatóknak az illetékes hatóságok által elektronikusan aláírt dokumentumokat kell benyújtaniuk.

(2) Az eljárásoknak a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv szerinti egyablakos ügyintézési pontokon keresztül elektronikus eszközökkel történő teljesítését lehetővé tevő rendelkezések meghatározásáról szóló, 2009. október 16-i 2009/767/EK bizottsági határozat [2] lehetővé tette a minősített tanúsítvánnyal kísért, fokozott biztonságú elektronikus aláírás határon átnyúló használatát, valamint többek között arra kötelezte a tagállamokat, hogy mielőtt a szolgáltatóktól elektronikus aláírásokat kérnek be, végezzenek kockázatelemzéseket, illetve dolgozzanak ki szabályokat a minősített tanúsítványon alapuló, biztonságos aláírás-létrehozó eszközzel vagy anélkül létrehozott, fokozott biztonságú elektronikus aláírások tagállamok általi elfogadásáról. A 2009/767/EK határozat azonban nem állapítja meg, hogy az elektronikus aláírások mely formátumai alkalmazhatók az illetékes hatóságok által kiállított azon dokumentumokban, amelyeket a szolgáltatóknak a vonatkozó eljárások és alaki követelmények teljesítése során be kell nyújtaniuk.

(3) Tekintve, hogy a tagállami illetékes hatóságok a dokumentumok elektronikus aláírásakor jelenleg a fokozott biztonságú elektronikus aláírások többféle formátumát alkalmazzák, a bekérő tagállamoknak a dokumentumok feldolgozása során technikai nehézségeket okozhat a használt aláírási formátumok sokfélesége. Mivel a szolgáltatók számára lehetővé kell tenni az országhatáron átnyúló eljárások, illetve alaki követelmények elektronikus úton való teljesítését, gondoskodni kell róla, hogy a tagállamok a különböző formátumú fokozott biztonságú elektronikus aláírásoknak legalább egy részét technikailag kezelni tudják, amikor elektronikusan aláírt dokumentumokat kapnak más tagállamok illetékes hatóságaitól. Ha megállapításra kerülnek a fokozott biztonságú elektronikus aláírások azon formátumai, amelyeket a bekérő tagállamoknak technikailag fel kell tudniuk dolgozni, az fokozott automatizálást tesz lehetővé, és javítja az elektronikus folyamatok országhatárokon átnyúló interoperabilitását.

(4) Ha egy tagállam illetékes hatóságai az általában megszokottól eltérő elektronikus aláírási formátumot alkalmaznak, akkor valószínűleg bevezettek olyan ellenőrzési eszközöket is, amelyek révén aláírásaik a határokon túl is ellenőrizhetők. Ebben az esetben az ellenőrzési eszközökről – hogy a bekérő tagállam is igénybe vehesse azokat – könnyen hozzáférhető módon tájékoztatást kell nyújtani, kivéve, ha az ellenőrzéshez szükséges információkat maga az elektronikus dokumentum, az elektronikus aláírás vagy az elektronikus dokumentum hordozója tartalmazza.

(5) Ez a határozat nem érinti az eredeti példány, a hiteles másolat, illetve a hiteles fordítás fogalmának tagállami meghatározását. A határozat célja kizárólag az, hogy lehetővé tegye az elektronikus aláírások ellenőrzését azokban az eredeti példányokban, hiteles másolatokban és hiteles fordításokban, amelyeket a szolgáltatóknak az egyablakos ügyintézési pontokon keresztül esetleg be kell nyújtaniuk.

[1] HL L 376., 2006.12.27., 36. o.
[2] HL L 274., 2009.10.20., 36. o.

(6) Annak érdekében, hogy a tagállamok kiépíthessék a szükséges technikai eszközöket, helyénvaló, hogy e határozat 2011. augusztus 1-jétől legyen alkalmazandó.

(7) Az e határozatban előírt intézkedések összhangban vannak a szolgáltatási irányelvvel foglalkozó bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Referenciaformátum elektronikus aláírásokhoz

(1) A tagállamok meghozzák az ahhoz szükséges technikai intézkedéseket, hogy fel tudják dolgozni azokat az elektronikusan aláírt dokumentumokat, amelyeket a szolgáltatók az eljárások és alaki követelmények teljesítése során a 2006/123/EK irányelv 8. cikkének megfelelően egyablakos ügyintézési pontokon keresztül nyújtanak be, és amelyeket más tagállamok illetékes hatóságai a mellékletben megadott technikai előírásokkal összhangban BES vagy EBES típusú, fokozott biztonságú, XML, CMS vagy PDF formátumú elektronikus aláírással láttak el.

(2) Azoknak a tagállamoknak, amelyeknek illetékes hatóságai az (1) bekezdésben említett dokumentumokat az ugyanazon bekezdésben említettektől eltérő formátumú elektronikus aláírással látják el, tájékoztatniuk kell a Bizottságot arról, hogy más tagállamok milyen ingyenes online, nem anyanyelvi beszélők számára is érthető ellenőrzési lehetőségek révén bizonyosodhatnak meg a kapott elektronikus aláírások hitelességéről, kivéve, ha a szükséges információ már szerepel a dokumentumban, az elektronikus aláírás mellett vagy az elektromos dokumentum hordozóján. A Bizottság ezeket az információkat közölni fogja mindegyik tagállammal.

2. cikk

Alkalmazás

Ezt a határozatot 2011. augusztus 1-jétől kell alkalmazni.

3. cikk

Címzettek

Ennek a határozatnak a tagállamok a címzettjei.

Kelt Brüsszelben, 2011. február 25-én.

a Bizottság részéről

Michel BARNIER

a Bizottság tagja

MELLÉKLET

A bekérő tagállamban technikai feldolgozásra kötelezően alkalmas, XML, CMS, illetve PDF formátumú, fokozottan biztonságos elektronikus aláírás jellemzői

A dokumentum következő részében a KÖTELEZŐ, a TILOS, a SZÜKSÉGES, a KELL, a TILOS/TILTOTT, a JAVASOLT, a NEM JAVASOLT, az AJÁNLOTT, a LEHET és az OPCIONÁLIS értelmezésére az RFC 2119-ben [1] leírtak irányadók.

1. RÉSZ – XAdES-BES/EPES

Az aláírás megfelel a W3C XML aláírási szabványnak [2].

Az aláírásnak KÖTELEZŐ legalább az ETSI TS 101 903 XAdES szabvány [3] szerinti XAdES-BES (vagy -EPES) formátumúnak lennie, és ki kell elégítenie az összes alábbi követelményt is:

A „ds:CanonicalizationMethod" parancs, amely az aláírási számítások elvégzése előtt meghatározza a „SignedInfo" elemre alkalmazandó kanonizációs algoritmust, kizárólag az alábbi algoritmusok egyikét választhatja ki:

Kanonikus XML 1.0 (megjegyzések nélkül):	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Kanonikus XML 1.1 (megjegyzések nélkül):	http://www.w3.org/2006/12/xml-c14n11
Kizárólagos XML kanonizáció 1.0 (megjegyzések nélkül):	http://www.w3.org/2001/10/xml-exc-c14n#

Az aláírás létrehozása során NEM JAVASOLT más algoritmusok, illetve az előbb felsorolt algoritmusok „megjegyzésekkel" ellátott verzióinak alkalmazása, de ezeket az algoritmusokat a reziduális interoperabilitás szintjéig JAVASOLT támogatni az aláírás ellenőrzéséhez.

Az MD5 (RFC 1321) algoritmust TILOS „digest algoritmusként" alkalmazni. Az aláírók vegyék figyelembe az alkalmazandó nemzeti jogszabályokat, illetve iránymutatásért olvassák el az ETSI TS 102 176 szabványt [4], valamint az ECRYPT2 D.SPA.x jelentést [5], ahol további javaslatokat találnak az elektronikus aláírásoknál használható algoritmusokról és paraméterekről.

Transzformációs algoritmusként kizárólag az alább felsoroltak alkalmazhatók:

Kanonizációs transzformációk (átalakítási leírások): lásd a kapcsolódó fenti specifikációt

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

Szűrés:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): kompatibilitási okok miatt és az XMLDSig-nek való megfelelés érdekében

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): teljesítménybeli gondokat követően az XPath utódja

***Enveloped signature* (XML-be ágyazott aláírás) transzformáció:** (http://www.w3.org/2000/09/xmldsig#enveloped-signature)

XSLT (style sheet) **transzformáció**

A „ds:KeyInfo" elemnek KÖTELEZŐ tartalmaznia az aláíró X.509 v3 digitális tanúsítványát (azaz magát az értéket, nem csupán az arra vonatkozó hivatkozást)

A „SigningCertificate" aláírt aláírási jellemzőnek KÖTELEZŐ tartalmaznia „digest value" értéket (CertDigest) és a „ds:KeyInfo" alatt tárolt aláírói tanúsítványban szereplő „IssuerSerial" sorszámot, viszont TILOS a „SigningCertificate" mezőben szereplő opcionális URI (egységes erőforrás-azonosító) használata

A „SigningTime" aláírt aláírási jellemző fel van tüntetve, és tartalmazza az „xsd:dateTime" algoritmus formájában megadott UTC-t (koordinált világidőt) (http://www.w3.org/TR/xmlschema-2/#dateTime)

A „DataObjectFormat" elemet KÖTELEZŐ feltüntetni, és tartalmaznia kell a „MimeType" alelemet.

Amennyiben a tagállamok által használt aláírások minősített tanúsítványon alapulnak, az aláírásban szereplő PKI-elemek (tanúsítási láncok, visszavonási adatok, időbélyegek) a 2009/767/EK határozattal összhangban ellenőrizhetők az aláíró tanúsítványát kibocsátó CSP-t (hitelesítés szolgáltatót) ellenőrző és akkreditáló tagállam megbízhatósági listája (Trusted List) alapján.

Az 1. táblázat összefoglalja a XAdES-BES/EPES formátumú aláírás által kielégítendő követelményeket, amelyeket teljesíteni kell ahhoz, hogy a bekérő tagállam az aláírást technikailag fel tudja dolgozni.

---

[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] Legutolsó verzió: D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), 2010. március 30. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

1. táblázat

XAdES - BES (EPES)		**Közös minimumkövetelmények**
(Az ETSI TS 103 903 szabványt az alább meghatározott elemekkel kell alkalmazni)		
K = kötelező; O = opcionális; A = ajánlott; N = nem alkalmazandó		
ds: Signature ID	**K**	
ds: SignedInfo	**K**	
ds: CanonicalizationMethod	**K**	***Az alábbi algoritmusok mindegyikét KÖTELEZŐ támogatni az aláírás ellenőrzéséhez, az aláírás létrehozásakor JAVASOLT az alábbiak egyikére korlátozni az alkalmazást:*** ***- kizárólagos XML kanonizáció 1.0: http://www.w3.org/TR/xml-exc-c14n/*** ***- kanonikus XML 1.0: http://www.w3.org/TR/2001/REC-XML-c14n-20010315*** ***- kanonikus XML 1.1: http://www.w3.org/2006/12/xml-c14n11*** ***Egyéb algoritmusok, illetve a fenti algoritmusok megjegyzésekkel ellátott (#WithComments) verzióinak alkalmazása NEM JAVASOLT.***
ds: SignatureMethod	**K**	***Algoritmusok:** lásd az alkalmazandó nemzeti jogszabályokat, valamint iránymutatásért az ETSI TS 102 176 szabványt, illetve további javaslatokért az ECRYPT2 D.SPA.7 jelentést.*
ds: Reference URI	**K**	**Egy hivatkozás mindegyik aláírandó eredeti adatobjektumra (az URI-k mutathatnak külső objektumra is) + hivatkozás a *SignedProperties* elemre**
ds: Transforms	**O**	***Az ellenőrző alkalmazásoknak KÖTELEZŐ támogatniuk az alábbi átalakítási leírások (transzformációk) mindegyikét, míg az aláírást létrehozó alkalmazásnak az említett transzformációk használatát JAVASOLT az alábbiakra korlátoznia:*** ***- Kanonizációs transzformációk: lásd fent*** ***- Base64 kódolás*** ***- XPath és XPath Filter 2.0*** ***- Enveloped signature transzformáció*** ***- XSLT transzformációk***
ds: DigestMethod	**K**	***Algoritmusok:** lásd az alkalmazandó nemzeti jogszabályokat, valamint iránymutatásért az ETSI TS 102 176 szabványt, illetve további javaslatokért az ECRYPT2 D.SPA.7 jelentést.*
ds: DigestValue	**K**	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	**K**	
ds: KeyInfo	**K**	**KÖTELEZŐ tartalmaznia az X509 tanúsítványt (a SigningCertificate aláírási attribútumnak KÖTELEZŐ tartalmaznia az aláírói tanúsítvány digest value értékét)** **JAVASOLT az aláírói tanúsítvány tanúsítási láncának feltüntetése utalásként az ellenőrzési folyamat megkönnyítése érdekében (ebben az esetben az X.509 tanúsítványt KÖTELEZŐ megadni).**
ds: Object		
QualifyingProperties	**K**	
SignedProperties	**K**	**K**
SignedSignatureProperties	**K**	**K**
SigningTime	**K**	**UTC (xsd: dateTime).**
SigningCertificate	**K**	**KÖTELEZŐ tartalmaznia az aláírói tanúsítvány ds:KeyInfo alatt szereplő digest value értékét, a tetszőleges URI-t viszont ki kell hagyni (előfordulhat, hogy az alkalmazások a hash megfelelés alapján a ds:KeyInfo alatt keresik/találják az aláírói tanúsítványt).**
SignaturePolicyIdentifier	**O**	**csak az EPES formátum elfogadott (és az EPES formátumra épülő továbbfejlesztett formátumok)**
Signature ProductionPlace	**O**	
SignerRole	**O**	
/SignedSignatureProperties		
SignedDataObjectProperties	**O**	
DataObjectFormat	**K**	**Ennek a mezőnek a használata esetén az alkalmazásoknak az adatobjektumokat ennek megfelelően KELL feltüntetniük a felhasználó számára.** **Ha használják, KÖTELEZŐ MimeType típusú gyermek elemet alkalmazni.**
CommitmentTypeIndication	**O**	
AllDataObjectsTimeStamp	**O**	
IndividualDataObjectTimeStamp	**O**	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	**O**	
UnsignedSignatureProperties		
CounterSignature	**O**	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Aláírástopológia - aláírt eredeti fájlok és aláírások tömörítése		
SignatureEnveloped		**Ezek mindegyikét KÖTELEZŐ támogatni**
SignatureEnveloping		
SignatureDetached		

2. RÉSZ – CAdES-BES/EPES

Az aláírásnak teljesítenie kell a „Cryptographic Message Syntax” (CMS) szerinti aláírási követelményeket ([1]).

Az aláírás az ETSI TS 101 733 CAdES szabványban ([2]) meghatározott CAdES-BES (vagy -EPES) aláírási attribútumokat alkalmazza, és teljesíti az alábbi 2. táblázatban foglalt további követelményeket is.

A CAdES-nak az archív időbélyeg hash függvény által használt összes attribútumát (ETSI TS 101 733 V1.8.1, K. melléklet) KÖTELEZŐ DER-kódban megadni, a többi attribútum azonban a CAdES egymenetes feldolgozásának (one-pass processing) megkönnyítése érdekében lehet BER-kódolású.

Az MD5 (RFC 1321) algoritmust TILOS digest algoritmusként alkalmazni. Az aláírók vegyék figyelembe az alkalmazandó nemzeti jogszabályokat, illetve iránymutatásért olvassák el az ETSI TS 102 176 szabványt ([3]), valamint az ECRYPT2 D.SPA.x jelentést ([4]), ahol további javaslatokat találnak az elektronikus aláírásoknál használható algoritmusokról és paraméterekről.

Az aláírt attribútumoknak (signed attributes) KÖTELEZŐ hivatkozást tartalmazniuk az aláíró X.509 v3 digitális tanúsítványára (RFC 5035) és a *SignedData.certificates* mezőnek KÖTELEZŐ tartalmaznia a tanúsítvány értékét.

A „SigningTime” aláírt attribútumot KÖTELEZŐ feltüntetni, és annak KÖTELEZŐ tartalmaznia a http://tools.ietf.org/html/rfc5652#section-11.3 szerint kifejezett UTC-t (koordinált világidőt)

A „ContentType” aláírt attribútumot KÖTELEZŐ feltüntetni, és annak azonosító adatot is tartalmaznia kell (http://tools.ietf.org/html/rfc5652#section-4) abban az esetben, ha az adattartalom-típus elvileg tetszőleges „octet string”-ekre, például UTF-8 szövegre vagy „MimeType” alelemet tartalmazó tömörített ZIP-re hivatkozik.

Amennyiben a tagállamok által használt aláírások minősített tanúsítványon alapulnak, az aláírásban szereplő PKI-elemek (tanúsítási láncok, visszavonási adatok, időbélyegek) a 2009/767/EK határozattal összhangban ellenőrizhetők az aláíró tanúsítványát kibocsátó CSP-t (hitelesítés szolgáltatót) ellenőrző és akkreditáló tagállam megbízhatósági listája (Trusted List) alapján.

([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]) Legutolsó verzió: D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), 2010. március 30. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

2. táblázat

CAdES - BES (EPES)		**Közös minimumkövetelmények**
(Az ETSI TS 101 733 szabványt az alább meghatározott elemekkel kell alkalmazni)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
K = kötelező; O = opcionális; A = ajánlott; N = nem alkalmazandó		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	K	**Algoritmusok:** lásd az alkalmazandó nemzeti jogszabályokat, valamint iránymutatásért az ETSI TS 102 176 szabványt, illetve további javaslatokért az ECRYPT2 D.SPA.7 jelentést.
encapContentInfo SEQUENCE {		
eContentType ContentType,	K	Azonosító adat (id-data)
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	K/N	A ContentType aláírt attribútum fel van tüntetve és tartalmaz azonosító adatot (http://tools.ietf.org/html/rfc5652#section-4) abban az esetben, ha az adattartalom-típus tetszőleges octet string-ekre kíván hivatkozni, például UTF-8 szövegre vagy MimeType alelemet tartalmazó tömörített ZIP-re.
-- External Data (if signature detached)*		ha az aláírt tartalomtól különálló aláírás (detached signature) egyébként nincs feltüntetve. * A külső adat olyan adat, amelyet a CAdES aláírás eContent részében nem szereplő, különálló aláírás véd. Az aláírt külső adatokat érdemes az aláírással együtt egy ZIP-fájlba tömöríteni.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	K	KÖTELEZŐ tartalmaznia az aláíró X509 tanúsítványát. JAVASOLT a tanúsítási lánc mentén az összes tanúsítvány feltüntetése a legfelsőbb szintű hitelesítés szolgáltatóig (trust anchor).
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	O	
signerInfos SET OF	K	Legalább egy signerinfo
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	O	(Nem védett érték)
digestAlgorithm DigestAlgorithmIdentifier,	K	**Algoritmusok:** lásd az alkalmazandó nemzeti jogszabályokat, valamint iránymutatásért az ETSI TS 102 176 szabványt, illetve további javaslatokért az ECRYPT2 D.SPA.7 jelentést.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	K	
attrType OBJECT IDENTIFIER,	K/O	KÖTELEZŐ: id-contentType (azonosító adattal) id-messageDigest id-aa-ets-signingCertificateV2 vagy id-aa-signingCertificate KÖTELEZŐ: signingTime OPCIONÁLIS: id-aa-ets-sigPolicyId Az ETSI TS 101 733 szerinti egyéb opcionális attribútumok.
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmusok:** lásd az alkalmazandó nemzeti jogszabályokat, valamint iránymutatásért az ETSI TS 102 176 szabványt, illetve további javaslatokért az ECRYPT2 D.SPA.7 jelentést.
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	O	
SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }	O	

3. RÉSZ – PAdES-PART 3 (BES/EPES):

Az aláírásnak KÖTELEZŐ az ETSI TS 102 778 PAdES-Part3 szabványnak ([1]) megfelelő PAdES-BES (vagy -EPES) aláíráskiterjesztést kell használnia, és teljesítenie kell az alábbi kiegészítő követelményeket is:

Az MD5 (RFC 1321) algoritmust TILOS „digest algoritmusként” alkalmazni. Az aláírók vegyék figyelembe az alkalmazandó nemzeti jogszabályokat, illetve iránymutatásért olvassák el az ETSI TS 102 176 szabványt ([2]), valamint az ECRYPT2 D.SPA.x jelentést ([3]), ahol további javaslatokat találnak az elektronikus aláírásoknál használható algoritmusokról és paraméterekről.

Az aláírt attribútumoknak (signed attributes) KÖTELEZŐ hivatkozást tartalmazniuk az aláíró X.509 v3 digitális tanúsítványára (RFC 5035) és a *SignedData.certificates* mezőnek KÖTELEZŐ tartalmaznia a tanúsítvány értékét.

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

Az aláírás időpontját az aláírási jegyzékben (signature dictionary) szereplő M bejegyzés értéke jelzi

Amennyiben a tagállamok által használt aláírások minősített tanúsítványon alapulnak, az aláírásban szereplő PKI-elemek (tanúsítási láncok, visszavonási adatok, időbélyegek) a 2009/767/EK határozattal összhangban ellenőrizhetők az aláíró tanúsítványát kibocsátó CSP-t (hitelesítés szolgáltatót) ellenőrző és akkreditáló tagállam megbízhatósági listája (Trusted List) alapján.