ROZHODNUTÍ

ROZHODNUTÍ KOMISE

ze dne 25. února 2011,

kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu

(oznámeno pod číslem K(2011) 1081)

(Text s významem pro EHP)

(2011/130/EU)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady 2006/123/ES ze dne 12. prosince 2006 o službách na vnitřním trhu [1], a zejména na čl. 8 odst. 3 této směrnice,

vzhledem k těmto důvodům:

(1) Poskytovatelé služeb, jejichž služby spadají do oblasti působnosti směrnice 2006/123/ES, musí být prostřednictvím jednotných kontaktních míst a elektronickými prostředky schopni splnit postupy a formality potřebné pro přístup k jejich činnostem a jejich výkonu. V mezích stanovených v čl. 5 odst. 3 směrnice 2006/123/ES se nadále mohou vyskytovat případy, kdy poskytovatelé služeb musí při plnění takových postupů a formalit předkládat originály dokumentů, ověřené kopie nebo ověřené překlady dokumentů. V takových případech může být nezbytné, aby poskytovatelé služeb předložili dokumenty elektronicky podepsané příslušnými orgány.

(2) Přeshraniční využití zaručených elektronických podpisů založených na kvalifikovaném osvědčení je usnadněno rozhodnutím Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu [2], jež mimo jiné ukládá členským státům povinnost provést posouzení rizik před vyžádáním těchto elektronických podpisů od poskytovatelů služeb a stanoví pravidla pro přijímání zaručených elektronických podpisů založených na kvalifikovaném osvědčení členskými státy, ať již byly vytvořeny prostředky pro bezpečné vytváření podpisu, či ne. Rozhodnutí 2009/767/ES se však nezabývá formáty elektronických podpisů v dokumentech vydaných příslušnými orgány, které musí poskytovatelé služeb při plnění příslušných postupů a formalit předložit.

(3) Vzhledem k tomu, že příslušné orgány v členských státech v současné době používají k elektronickému podepsání svých dokumentů různé formáty zaručených elektronických podpisů, mohou se přijímající členské státy, které musí tyto dokumenty zpracovat, v důsledku různých použitých formátů podpisu potýkat s technickými obtížemi. Aby mohli poskytovatelé služeb plnit postupy a formality elektronickou cestou i přes hranice, je nutné zajistit, aby členské státy při přijímání dokumentů elektronicky podepsaných příslušnými orgány z jiných členských států technicky podporovaly alespoň některé formáty zaručených elektronických podpisů. Definování určitého počtu zaručených elektronických podpisů, které mají být technicky podporovány přijímajícím členským státem, by umožnilo větší automatizaci a zlepšení přeshraniční interoperability elektronických postupů.

(4) Členské státy, jejichž příslušné orgány používají jiné formáty elektronického podpisu, než jaké jsou běžně podporovány, mohly zavést ověřovací prostředky umožňující ověření těchto podpisů i za hranicemi. V takovém případě je nutné, aby informace o těchto nástrojích byly snadno přístupné (pokud potřebné informace nejsou obsaženy přímo v elektronických dokumentech, elektronických podpisech nebo nosičích elektronických dokumentů) tak, aby se přijímající členské státy mohly na tyto ověřovací nástroje spolehnout.

(5) Toto rozhodnutí nemá vliv na stanovení toho, co představuje originál, ověřenou kopii nebo ověřený překlad ze strany členských států. Jeho cíl se omezuje na usnadnění ověřování elektronických podpisů, pokud jsou použity v originálech, ověřených kopiích nebo ověřených překladech, které mají poskytovatelé služeb předložit prostřednictvím jednotných kontaktních míst.

[1] Úř. věst. L 376, 27.12.2006, s. 36.
[2] Úř. věst. L 274, 20.10.2009, s. 36.

(6) S cílem umožnit členským státům zavedení nezbytných technických nástrojů je vhodné, aby se toho rozhodnutí použilo od 1. srpna 2011.

(7) Opatření tohoto rozhodnutí jsou v souladu se stanoviskem výboru pro směrnici o službách,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Referenční formát elektronických podpisů

1. Členské státy zavedou nezbytné technické prostředky, které jim umožní zpracování elektronicky podepsaných dokumentů, jež v rámci plnění postupů a formalit předkládají poskytovatelé služeb prostřednictvím jednotných kontaktních míst, jak je stanoveno v článku 8 směrnice 2006/123/ES, a které jsou podepsány příslušnými orgány jiných členských států pomocí zaručeného elektronického podpisu XML nebo CMS nebo PDF ve formátu BES nebo EPES, který je v souladu s technickými specifikacemi uvedenými v příloze.

2. Členské státy, jejichž příslušné orgány podepisují dokumenty uvedené v odstavci 1 za použití jiných formátů elektronických podpisů, než jsou uvedeny v odstavci 1, oznámí Komisi stávající možnosti ověření, které umožní ostatním členským státům ověřit obdržené elektronické podpisy online, bez poplatku a způsobem, který je srozumitelný pro nerodilé mluvčí, pokud požadované informace nejsou již zahrnuty v dokumentu, elektronickém podpise nebo nosiči elektronického dokumentu. Komise zpřístupní tyto informace všem členským státům.

Článek 2

Použití

Toto rozhodnutí se použije od 1. srpna 2011.

Článek 3

Určení

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 25. února 2011.

Za Komisi
Michel BARNIER
člen Komise

PŘÍLOHA

Specifikace pro zaručený elektronický podpis XML, CMS nebo PDF, který má být technicky podporován přijímajícím členským státem

V následující části tohoto dokumentu se klíčové výrazy „MUSÍ“, „NESMÍ“, „POVINNÝ“, „MĚL BY“, „NEMĚL BY“, „DOPORUČUJE SE“, „MŮŽE“ a „VOLITELNÝ“ mají vykládat v souladu s RFC 2119 ([1]).

ODDÍL 1 – XAdES-BES/EPES:

Podpis je v souladu se specifikacemi W3C pro podpis XML (*W3C XML Signature specifications*) ([2])

Podpis MUSÍ mít alespoň formát XAdES-BES (nebo -EPES), jak je uvedeno ve specifikacích ETSI TS 101 903 XAdES ([3]), a být v souladu se všemi následujícími dalšími specifikacemi:

Ds:CanonicalizationMethod, která určuje kanonizační algoritmus použitý na element *SignedInfo* před provedením výpočtu podpisu, určuje pouze jeden z následujících algoritmů:

Canonical XML 1.0 (vynechává komentáře): http://www.w3.org/TR/2001/REC-xml-c14n-20010315

Canonical XML 1.1 (vynechává komentáře): http://www.w3.org/2006/12/xml-c14n11

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

Jiné algoritmy nebo verze „s komentáři“ výše uvedených algoritmů BY se NEMĚLY používat pro vytvoření podpisu, ale MĚLY by být podporovány pro ověření podpisu v rámci zbytkové interoperability.

MD5 (RFC 1321) se NESMÍ použít jako hašovací (*digest*) algoritmus. Další doporučení týkající se alogoritmů a parametrů způsobilých pro elektronické podpisy mohou podepisující subjekty nalézt v platných vnitrostátních předpisech a pro účely pokynů v technických specifikacích ETSI TS 102 176 ([4]) a zprávě ECRYPT2 D.SPA.x ([5]).

Použití *transformací* je omezeno na níže uvedené:

Kanonizační transformace: viz související specifikace uvedené výše;

Kódování base64 (http://www.w3.org/2000/09/xmldsig#base64);

Filtrování:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): z důvodů kompatibility a souladu s XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): jako nástupce XPath kvůli problémům s výkonem

Transformace podpisu *Enveloped signature*: (http://www.w3.org/2000/09/xmldsig#enveloped-signature).

Transformace XSLT (stylový předpis).

Element *ds:KeyInfo* MUSÍ obsahovat digitální osvědčení X.509 v3 podepisujícího (tj. jeho hodnotu, a ne pouze odkaz na ni).

Podepsaný atribut podpisu „*SigningCertificate*“ MUSÍ obsahovat hašovací (*digest*) hodnotu (*CertDigest*) a *IssuerSerial* osvědčení podepisujícího uloženého v *ds:KeyInfo* a volitelný URI v poli „*SigningCertificate*“ se NESMÍ použít.

Podepsaný atribut *SigningTime* podpisu je přítomen a obsahuje koordinovaný světový čas (UTC) vyjádřený jako *xsd:dateTime* (http://www.w3.org/TR/xmlschema-2/#dateTime).

Element *DataObjectFormat* MUSÍ být přítomen a obsahovat sub-element *MimeType*;

Pokud jsou podpisy používané v členských státech založené na kvalifikovaném osvědčení, objekty PKI (řetězce osvědčení, údaje o odvolání, časové značky), jež jsou zahrnuty v podpisech, jsou podle rozhodnutí Komise 2009/767/ES ověřitelné pomocí důvěryhodného seznamu členského státu, který vykonává dohled nad ověřovateli, jež vydali osvědčení podepisující osoby, nebo je akredituje.

Tabulka 1 shrnuje specifikace, se kterými musí být podpis XAdES-BES/EPES v souladu, aby mohl být přijímajícím členským státem technicky podporován.

([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; Část 1: Hash functions and asymmetric algorithms; Část 2: „Secure channel protocols and algorithms for signature creation devices“.
([5]) Nejnovější verze je D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010) ze dne 30. března 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabulka 1

XAdES - BES (EPES)		**Společné minimální požadavky**
(ETSI TS 103 903 se použije s těmito profilovanými elementy)		
M = povinné; O = volitelné; R = doporučené; N = nepoužije se		
ds: Signature ID	**M**	
ds: SignedInfo	**M**	
ds: CanonicalizationMethod	**M**	***Všechny tyto algoritmy musí být podporovány pro ověření podpisu, vytváření BY se MĚLO omezit na jeden z těchto algoritmů:*** ***- 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-c1***
ds: SignatureMethod	**M**	***Algoritmy: další doporučení lze nalézt v platných vnitrostátních předpisech a pro účely pokynů ve specifikacích ETSI TS 102 176 a ve zprávě ECRYPT2 D.SPA.7 .***
ds: Reference URI	**M**	**Jeden odkaz na každý původní datový objekt, který má být podepsán (URI mohou rovněž odkazovat na externí objekt), + odkaz na element SignedProperties**
ds: Transforms	**O**	***Aplikace pro ověření MUSÍ podporovat všechny následující transformace, zatímco aplikace pro vytváření podpisů BY MĚLA omezit používání transformací na tyto:*** ***- Kanonizační transformace: viz výše*** ***- Kódování Base64*** ***- XPath a XPath Filter 2.0*** ***- Transforma***
ds: DigestMethod	**M**	***Algoritmy: další doporučení lze nalézt v platných vnitrostátních předpisech a pro účely pokynů ve specifikacích ETSI TS 102 176 a ve zprávě ECRYPT2 D.SPA.7.***
ds: DigestValue	**M**	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	**M**	
ds: KeyInfo	**M**	**MUSÍ obsahovat osvědčení X509 (podepsaný atribut SigningCertificate MUSÍ obsahovat hašovací hodnotu osvědčení této podepisující osoby)** **DOPORUČUJE SE poskytnout certifikační řetězec osvědčení podepisující osoby pro usnadnění procesu ověřování (osvědčení X**
ds: Object		
QualifyingProperties	**M**	
SignedProperties	**M**	**M**
SignedSignatureProperties	**M**	**M**
SigningTime	**M**	**UTC (xsd: dateTime).**
SigningCertificate	**M**	**MUSÍ obsahovat hašovací hodnotu osvědčení podepisujícího uloženého v ds:KeyInfo a volitelný URI je vynechán (Aplikace MŮŽE vyhledat/nalézt osvědčení podepisující osoby v ds:KeyInfo na základě rovnosti hašů).**
SignaturePolicyIdentifier	**O**	**pouze formát EPES a pro vyšší formáty sestavené z formátu EPES)**
Signature ProductionPlace	**O**	
SignerRole	**O**	
/SignedSignatureProperties		
SignedDataObjectProperties	**O**	
DataObjectFormat	**M**	**Při použití tohoto pole MUSÍ aplikace zajistit, aby se datové objekty uživateli zobrazily odpovídajícím způsobem.** **Je-li použit, MUSÍ se použít podřízený element MimeType.**
CommitmentTypeIndication	**O**	
AllDataObjectsTimeStamp	**O**	
IndividualDataObjectTimeStamp	**O**	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	**O**	
UnsignedSignatureProperties		
CounterSignature	**O**	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Topologie podpisu: Zapouzdření podepsaných původních souborů a podpisů		
SignatureEnveloped		**Všechny MUSÍ být podporovány**
SignatureEnveloping		
SignatureDetached		

ODDÍL 2 – CAdES-BES/EPES

Podpis je v souladu se specifikacemi *Cryptographic Message Syntax (CMS) Signature* [1]

Podpis používá podpisové atributy CAdES-BES (nebo -EPES), jak je uvedeno ve specifikacích ETSI TS 101 733 CAdES [2], a je v souladu s dalšími specifikacemi, jak je uvedeno níže v tabulce 2.

Všechny atributy CAdES, jež jsou zahrnuty do výpočtu archivní časové značky haše (ETSI TS 101 733 V1.8.1 příloha K), MUSÍ být v kódování DER a všechny ostatní atributy mohou být v BER pro zjednodušení jednofázového zpracování CAdES.

MD5 (RFC 1321) se NESMÍ použít jako hašovací (*digest*) algoritmus. Další doporučení týkající se algoritmů a parametrů způsobilých pro elektronické podpisy mohou podepisující subjekty nalézt v platných vnitrostátních předpisech a pro účely pokynů v technických specifikacích ETSI TS 102 176 [3] a ve zprávě ECRYPT2 D.SPA.x [4].

Podepsané atributy MUSÍ obsahovat odkaz na digitální osvědčení X.509 v3 podepisující osoby (RFC 5035) a pole *SignedData.certificates* MUSÍ obsahovat jeho hodnotu;

Podepsaný atribut *SigningTime* MUSÍ být přítomen a MUSÍ obsahovat UTC vyjádřený podle http://tools.ietf.org/html/rfc5652#section-11.3.

Podepsaný atribut *ContentType* MUSÍ být přítomen a obsahovat id-data (http://tools.ietf.org/html/rfc5652#section-4), kde typ obsahu dat má odkazovat na sekvence libovolných oktetů, jako je text UTF-8 nebo ZIP archiv (*container*) se sub-elementem *MimeType*.

Pokud jsou podpisy používané členskými státy založené na kvalifikovaném osvědčení, objekty PKI (řetězce osvědčení, údaje o odvolání, časové značky), jež jsou zahrnuty v podpisech, jsou podle rozhodnutí Komise 2009/767/ES ověřitelné pomocí důvěryhodného seznamu členského státu, který vykonává dohled nad ověřovateli, jež vydali osvědčení podepisující osoby, nebo je akredituje.

[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; Část 1: Hash functions and asymmetric algorithms; Část 2: „Secure channel protocols and algorithms for signature creation device".

[4] Nejnovější verze je D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010) ze dne 30. března 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabulka 2

CAdES - BES (EPES)		Společné minimální požadavky
(ETSI TS 101 733 se použije s těmito profilovanými elementy)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
M = povinné; O = volitelné; R = Doporučené; N = Nepoužije se		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	M	**Algoritmy:** další doporučení lze nalézt v platných vnitrostátních předpisech a pro účely pokynů ve specifikacích ETSI TS 102 176 a ve zprávě ECRYPT2 D.SPA.7.
encapContentInfo SEQUENCE {		
eContentType ContentType,	M	id-Data
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	M/N	Podepsaný atribut ContentType je přítomen a obsahuje id-data (http://tools.ietf.org/html/rfc5652#section-4), kde typ obsahu dat má odkazovat na sekvence libovolných oktetů, jako je text UTF-8 nebo ZIP archiv se sub-elementem MimeType
-- External Data (if signature detached)*		pokud oddělený podpis není jinak přítomen. * Externími daty se rozumí data chráněná odděleným podpisem, který není zahrnut v eContentu podpisu CAdES. Doporučuje se zahrnout podepsaná externí data spolu s podpisem do souboru ZIP.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	M	MUSÍ obsahovat osvědčení X509 od podepisující osoby. DOPORUČUJE SE zahrnout osvědčení z celého certifikačního řetězce až po "pevný bod důvěry".
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	O	
signerInfos SET OF	M	Alespoň jeden element signerInfo
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	O	(Nechráněná hodnota)
digestAlgorithm DigestAlgorithmIdentifier,	M	**Algoritmy:** další doporučení lze nalézt v platných vnitrostátních předpisech a pro účely pokynů ve specifikacích ETSI TS 102 176 a ve zprávě ECRYPT2 D.SPA.7.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	M	
attrType OBJECT IDENTIFIER,	M/O	**MUSÍ:** id-contentType (s id daty) id-messageDigest id-aa-ets-signingCertificateV2 or id-aa-signingCertificate **MUSÍ:** signingTime **VOLITELNÉ:** id-aa-ets-sigPolicyId další volitelné atributy jsou definovány v ETSI TS 101 733.
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmy:** další doporučení lze nalézt v platných vnitrostátních předpisech a pro účely pokynů ve specifikacích ETSI TS 102 176 a ve zprávě ECRYPT2 D.SPA.7.
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	O	

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

ODDÍL 3 – PAdES - ČÁST 3 (BES/EPES)

Podpis MUSÍ používat rozšíření podpisu CAdES-BES (nebo -EPES), jak je uvedeno ve specifikacích ETSI TS 102 778 PAdES-Part3 ([1]) a být v souladu s těmito dalšími specifikacemi:

MD5 (RFC 1321) se NESMÍ použít jako hašovací (*digest*) algoritmus. Další doporučení týkající se algoritmů a parametrů způsobilých pro elektronické podpisy mohou podepisující subjekty nalézt v platných vnitrostátních předpisech a pro účely pokynů v technických specifikacích ETSI TS 102 176 ([2]) a ve zprávě ECRYPT2 D.SPA.x ([3]).

Podepsané atributy MUSÍ obsahovat odkaz na digitální osvědčení X.509 v3 podepisující osoby (RFC 5035) a pole *SignedData.certificates* MUSÍ obsahovat jeho hodnotu.

([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; Část 1: Hash functions and asymmetric algorithms; Část 2: „Secure channel protocols and algorithms for signature creation devices".

([3]) Nejnovější verze je D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010) ze dne 30. března 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Doba podepsání je vyjádřena hodnotou hesla **M** v tzv. „slovníku podpisu“ (*signature dictionary*).

Pokud jsou podpisy používané členskými státy založené na kvalifikovaném osvědčení, objekty PKI (řetězce osvědčení, údaje o odvolání, časové značky), jež jsou zahrnuty v podpisech, jsou podle rozhodnutí Komise 2009/767/ES ověřitelné pomocí důvěryhodného seznamu členského státu, který vykonává dohled nad ověřovateli, jež vydali osvědčení podepisující osoby, nebo je akredituje.