ROZHODNUTIA

ROZHODNUTIE KOMISIE

z 25. februára 2011,

ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu

[oznámené pod číslom K(2011) 1081]

(Text s významom pre EHP)

(2011/130/EÚ)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na smernicu Európskeho parlamentu a Rady 2006/123/ES z 12. decembra 2006 o službách na vnútornom trhu [1], a najmä na jej článok 8 ods. 3,

keďže:

(1) Poskytovatelia služieb, ktorých služby patria do rozsahu pôsobnosti smernice 2006/123/ES, musia byť schopní prostredníctvom miest jednotného kontaktu a elektronickými prostriedkami plniť postupy a formality potrebné na prístup k ich činnostiam a na ich vykonávanie. V medziach ustanovených v článku 5 ods. 3 smernice 2006/123/ES môže stále dochádzať k prípadom, keď poskytovatelia služieb musia pri plnení takýchto postupov a formalít predkladať originály dokumentov, overené kópie alebo overené preklady. V takýchto prípadoch môže byť potrebné, aby poskytovatelia služieb predkladali dokumenty elektronicky podpísané príslušnými orgánmi.

(2) Cezhraničné používanie zaručených elektronických podpisov podporovaných kvalifikovaným osvedčením je uľahčené rozhodnutím Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu [2], ktorým sa okrem iného členským štátom ukladá povinnosť vykonávať hodnotenie rizík pred požadovaním týchto elektronických podpisov od poskytovateľov služieb a ktorým sa ustanovujú pravidlá uznávania zaručených elektronických podpisov založených na kvalifikovaných osvedčeniach členskými štátmi, vyhotovených na bezpečnom zariadení na vyhotovenie podpisu alebo bez tohto zariadenia. Rozhodnutie 2009/767/ES sa však nezaoberá formátmi elektronických podpisov v dokumentoch vydaných príslušnými orgánmi, ktoré musia predkladať poskytovatelia služieb pri plnení príslušných postupov a formalít.

(3) Keďže príslušné orgány v členských štátoch v súčasnosti používajú na elektronické podpisovanie svojich dokumentov rôzne formáty zaručených elektronických podpisov, prijímajúce členské štáty, ktoré majú spracúvať tieto dokumenty, môžu čeliť technickým problémom z dôvodu rozmanitosti používaných formátov podpisu. S cieľom umožniť poskytovateľom služieb plniť postupy a služby cezhranične elektronickými prostriedkami je potrebné zaistiť, aby členské štáty technicky podporovali aspoň niekoľko formátov zaručených elektronických podpisov, keď prijímajú dokumenty elektronicky podpísané príslušnými orgánmi z iných členských štátov. Určenie niekoľkých formátov zaručených elektronických podpisov, ktoré musia byť technicky podporované prijímajúcim členským štátom, by umožnilo väčšiu automatizáciu a zlepšenie cezhraničnej interoperability elektronických postupov.

(4) Členské štáty, ktorých príslušné orgány používajú iné formáty elektronických podpisov, ako sú bežne podporované, mohli zaviesť validačné prostriedky, ktoré umožnia, aby sa ich podpisy overovali cezhranične. Keď ide o takýto prípad a na to, aby sa prijímajúce členské štáty mohli spoliehať na tieto validačné nástroje, musia byť informácie o týchto nástrojoch ľahko dostupné, pokiaľ potrebné informácie nie sú uvedené priamo v elektronických dokumentoch, elektronických podpisoch alebo na nosičoch elektronických dokumentov.

(5) Týmto rozhodnutím sa neovplyvňuje to, ako členské štáty určia, čo tvorí originál, overenú kópiu alebo overený preklad. Cieľ tohto rozhodnutia sa obmedzuje na uľahčenie overovania elektronických podpisov, ak sa používajú v originálnych, overených kópiách alebo overených prekladoch, ktoré môžu poskytovatelia služieb potrebovať predložiť prostredníctvom miest jednotného kontaktu.

[1] Ú. v. EÚ L 376, 27.12.2006, s. 36.
[2] Ú. v. EÚ L 274, 20.10.2009, s. 36.

(6) S cieľom umožniť členským štátom zaviesť potrebné technické nástroje je vhodné, aby sa toto rozhodnutie uplatňovalo od 1. augusta 2011.

(7) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru zriadeného na základe smernice o službách,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Referenčný formát elektronických podpisov

1. Členské štáty zavedú potrebné technické prostriedky, ktoré im umožnia spracúvať elektronicky podpísané dokumenty, ktoré poskytovatelia služieb predkladajú v kontexte plnenia postupov a formalít prostredníctvom miest jednotného kontaktu, ako sa predpokladá v článku 8 smernice 2006/123/ES, a ktoré príslušné orgány ostatných členských štátov podpísali zaručeným elektronickým podpisom XML, CMS alebo PDF vo formáte BES alebo EPES, ktorý je v súlade s technickými špecifikáciami ustanovenými v prílohe.

2. Členské štáty, ktorých príslušné orgány podpisujú dokumenty uvedené v odseku 1, pričom používajú iné formáty elektronických podpisov, ako sú uvedené v rovnakom odseku, oznámia Komisii existujúce možnosti validácie, ktoré umožnia ostatným členským štátom validovať prijaté elektronické podpisy elektronicky, bezplatne a spôsobom, ktorý je zrozumiteľný pre cudzincov, pokiaľ sú požadované informácie už zahrnuté v dokumente, elektronickom podpise alebo na nosiči elektronických dokumentov. Komisia sprístupní tieto informácie všetkým členským štátom.

Článok 2

Uplatňovanie

Toto rozhodnutie sa uplatňuje od 1. augusta 2011.

Článok 3

Adresáti

Toto rozhodnutie je určené členským štátom.

V Bruseli 25. februára 2011

Za Komisiu

Michel BARNIER

člen Komisie

PRÍLOHA

Špecifikácie pre zaručený elektronický podpis XML, CMS alebo PDF, ktoré má prijímajúci členský štát technicky podporovať

V tejto časti dokumentu sa kľúčové slová „MUSÍ“, „NESMIE“, „POVINNÉ“, „BUDE“, „NEBUDE“, „MALO BY“, „NEMALO BY“, „ODPORÚČA SA“, „MÔŽE“ a „VOLITEĽNÉ“ majú vykladať v súlade s opisom uvedeným v RFC 2119 ([1]).

ODDIEL 1 – XAdES-BES/EPES

Tento podpis je v súlade so špecifikáciami podpisu W3C XML ([2]).

Podpis MUSÍ byť aspoň podpisovou formou XAdES-BES (alebo -EPES), ako je to uvedené v špecifikáciách ETSI TS 101903 XAdES ([3]), a MUSÍ vyhovovať všetkým týmto doplňujúcim špecifikáciám:

ds: Metóda kanonikalizácie, ktorá špecifikuje kanonikalizačný algoritmus, ktorý sa uplatňuje pri zložke SignedInfo ešte pred vykonaním výpočtu podpisu, identifikuje len jeden z týchto algoritmov:

Kanonický XML 1.0 (vynecháva pripomienky): http://www.w3.org/TR/2001/REC-xml-c14n-20010315.

Kanonický XML 1.1 (vynecháva pripomienky): http://www.w3.org/2006/12/xml-c14n11.

Exkluzívny XML kanonikalizácia 1.0 (vynecháva pripomienky): http://www.w3.org/2001/10/xml-exc-c14n#.

Ostatné algoritmy alebo verzie „with comments – s pripomienkami“ vyššie uvedených algoritmov BY SA NEMALI používať na vytváranie podpisov, ale BY MALI BYŤ podporované pre reziduálnu interoperabilitu na účely overenia podpisu.

MD5 (RFC 1321) sa NESMIE použiť ako hašovací algoritmus. Ďalšie odporúčania týkajúce sa algoritmov a parametrov, ktoré sa vzťahujú na elektronické podpisy, môžu podpisujúce subjekty nájsť v platných vnútroštátnych predpisoch a na účely usmernení v technických špecifikáciách ETSI TS 102176 ([4]) a v správe ECRYPT2 D.SPA.x ([5]).

Používanie *transformácií* je obmedzené na tie, ktoré sú uvedené nižšie:

Kanonikalizačné transformácie: pozri vyššie uvedené súvisiace špecifikácie.

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

Filtrovanie:

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

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): ako nástupca XPath z dôvodov výkonnosti.

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

Transformácia XSLT (štýly).

ds: zložka KeyInfo MUSÍ obsahovať digitálne osvedčenie podpisujúceho subjektu X.509 v3 (t. j. jeho hodnotu a nielen odkaz na ňu).

Atribút podpísaného podpisu SigningCertificate (osvedčenie o podpise) MUSÍ obsahovať hašovaciu hodnotu (CertDigest) a IssuerSerial osvedčenia podpisujúceho subjektu, ktoré sú uložené v ds:KeyInfo, a voliteľné URI v poli SigningCertificate sa NESMIE použiť.

Atribút podpísaného podpisu SigningTime (čas podpisu) musí byť prítomný a musí obsahovať UTC, ktoré je vyjadrené ako xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

Zložka DataObjectFormat MUSÍ byť prítomná a obsahovať pomocnú zložku MimeType.

V prípade, že sa podpisy, ktoré používajú členské štáty, zakladajú na kvalifikovanom osvedčení, objekty PKI (reťazce osvedčení, revokačné údaje, časové známky), ktoré sú obsiahnuté v podpisoch, sa v súlade s rozhodnutím Komisie 2009/767/ES dajú overiť prostredníctvom zoznamu dôveryhodných informácií členského štátu, ktorý kontroluje alebo akredituje CSP na základe vystavenia osvedčenia podpisujúceho subjektu.

Tabuľka 1 obsahuje zhrnutie špecifikácií, ktoré podpis XAdES-BES/EPES musí spĺňať na to, aby ho prijímajúci členský štát mohol technicky podporovať.

([1]) IETF RFC 2119: „Kľúčové slová, ktoré sa majú použiť v RFC a ktoré majú naznačovať úrovne požiadaviek“.

([2]) W3C, XML syntax a spracovanie podpisu, (verzia 1.1), http://www.w3.org/TR/xmldsig-core1/.
W3C, XML syntax a spracovanie podpisu, (druhé vydanie), http://www.w3.org/TR/xmldsig-core/
W3C, XML overené postupy podpisov, http://www.w3.org/TR/xmldsig-bestpractices/.

([3]) ETSI TS 101903 v1.4.1: XML zaručené elektronické podpisy (XAdES).

([4]) ETSI TS 102176: elektronické podpisy a infraštruktúra (ESI); algoritmy a parametre pre bezpečné elektronické podpisy; časť 1: Funkcie Hash a asymetrické algoritmy; časť 2: „Bezpečné kanálové protokoly a algoritmy pre zariadenia na vytváranie podpisov“.

([5]) Najnovšia verzia je D.SPA.13 ECRYPT2 Ročná správa o algoritmoch a kľúčových veľkostiach (2009 – 2010) z 30. marca 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabuľka 1

XAdES – BES (EPES)		**Spoločné minimálne požiadavky**
(ETSI TS 103 903 platí s nasledujúcimi profilovými prvkami)		
M = povinné; O = voliteľné; R = odporúčané; N = nepoužíva sa		
ds: Signature ID	M	
ds: SignedInfo	M	
ds: CanonicalizationMethod	M	*Každý z nasledujúcich algoritmov MUSÍ byť podporovaný kvôli overeniu podpisu, vytvorenie BY MALO BYŤ obmedzené na niektorý z nižšie uvedených algoritmov:* *– výlučne kanonikalizácia XML 1.0: http://www.w3.org/TR/xml-exc-c14n/* *– kanonikálny XML 1.0: http://www.w3.org/TR/2001/REC-XML-c14n-20010315* *– kanonikálny XML 1.1: http://www.w3.org/2006/12/xml-c14n11.* *Iné metódy alebo verzie "#WithComments" vyššie uvedených metód BY SA NEMALI používať.*
ds: SignatureMethod	M	***Algoritmy:*** *ďalšie odporúčania sa nachádzajú v platných vnútroštátnych právnych predpisoch a na účely pokynov v špecifikáciách ETSI TS 102 176 a správe ECRYPT2 D.SPA.7.*
ds: reference URI	M	Jeden odkaz na každý originálny dátový objekt na podpis (URI sa môžu týkať aj vonkajšieho objektu) + odkaz na prvok SignedProperties.
ds: Transforms	O	*Overovacie aplikácie MUSIA podporovať každú z nasledujúcich transformácií, pričom aplikácia vytvárania podpisu BY MALA obmedziť používanie transformácií na niektorú z uvedených:* *– kanonikalizačné transformery: pozri vyššie* *– kódovanie Base64* *– XPath a XPath Filter 2.0* *– transformácia podpisov (Enveloped signature transform)* *– transformácia XSLT.*
ds: DigestMethod	M	***Algoritmy:*** *ďalšie odporúčania sa nachádzajú v platných vnútroštátnych právnych predpisoch a na účely pokynov v špecifikáciách ETSI TS 102 176 a správe ECRYPT2 D.SPA.7.*
ds: DigestValue	M	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	M	
ds: KeyInfo	M	MUSÍ obsahovať osvedčenie X509 (riadne podpísaný SigningCertificate MUSÍ obsahovať digestívnu hodnotu osvedčenia autora tohto podpisu). Ako pomôcka na uľahčenie validačného procesu sa ODPORÚČA poskytnutie reťazca osvedčení k osvedčeniu podpisujúceho subjektu ako pripomienka na uľahčenie validačného postupu (v tomto prípade sa MUSIA predložiť osvedčenia X.509).
ds: Object		
QualifyingProperties	M	
SignedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC (xsd: dateTime).
SigningCertificate	M	MUSÍ obsahovať hašovaciu hodnotu osvedčenia autora podpisu uloženú v ds:KeyInfo, pričom voliteľné URI sa vynechá (aplikácie MÔŽU vyhľadávať/nájsť osvedčenie autora podpisu v ds:KeyInfo na základe kontrolnej zhody).
SignaturePolicyIdentifier	O	Len v prípade formulára EPES (a pre vyššie verzie vytvorené na základe formulára EPES).
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	M	V prípade použitia tohto políčka by aplikácie MALI zabezpečiť adekvátne zobrazenie dátových objektov pre používateľa. V prípade použitia tohto políčka MUSÍ byť použitý podriadený element MimeType.
CommitmentTypeIndication	O	
AllDataObjectsTimeStamp	O	
IndividualDataObjectTimeStamp	O	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	O	
UnsignedSignatureProperties		
CounterSignature	O	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Topológia podpisu – zabalenie podpísaných originálnych súborov a podpisov		
SignatureEnveloped		Všetky MUSIA byť podporované.
SignatureEnveloping		
SignatureDetached		

ODDIEL 2 – CAdES-BES/EPES

Tento podpis je v súlade so špecifikáciami týkajúcimi sa syntaxe podpisu kryptografických správ (CMS) ([1]).

Podpis využíva podpisové atribúty CAdES-BES (alebo -EPES), ako sa uvádza v špecifikáciách ETSI TS 101733 CAdES ([2]), a spĺňa doplňujúce špecifikácie, tak ako sa uvádza v tabuľke 2.

Všetky atribúty CAdES, ktoré sú uvedené v archíve výpočtu časovej známky hash (ETSI TS 101733 V1.8.1 príloha K), MUSIA byť zakódované formou DER a ostatné môžu mať formu BER, aby sa uľahčilo jednofázové spracovanie CAdES.

MD5 (RFC 1321) sa NESMIE použiť ako hašovací algoritmus. Ďalšie odporúčania týkajúce sa algoritmov a parametrov, ktoré sa vzťahujú na elektronické podpisy, môžu podpisujúce subjekty nájsť v platných vnútroštátnych predpisoch a na účely usmernení v technických špecifikáciách ETSI TS 102176 ([3]) a v správe ECRYPT2 D.SPA.x ([4]).

Podpísané atribúty MUSIA obsahovať odkaz na digitálne osvedčenie podpisujúceho subjektu X.509 v3 (RFC 5035) a kolónka *SignedData.certificates* (osvedčenia podpísaných údajov) MUSÍ obsahovať jeho hodnotu.

Podpísaný atribút SigningTime (čas podpisu) MUSÍ byť prítomný a MUSÍ obsahovať UTC, vyjadrené ako v http://tools.ietf.org/html/rfc5652#section-11.3;

Podpísaný atribút ContentType (typ obsahu) MUSÍ existovať a obsahovať id-data (http://tools.ietf.org/html/rfc5652#section-4), ak sa má typ obsahu vzťahovať na ľubovoľné oktetové reťazce, akým je text UTF-8 alebo objekt ZIP s pomocnou zložkou MimeType.

V prípade, že sa podpisy, ktoré používajú členské štáty, zakladajú na kvalifikovanom osvedčení, objekty PKI (reťazce osvedčení, revokačné údaje, časové známky), ktoré sú obsiahnuté v podpisoch, sa dajú overiť prostredníctvom zoznamu dôveryhodných informácií v súlade s rozhodnutím 2009/767/ES členského štátu, ktorý kontroluje alebo akredituje CSP na základe vystavenia osvedčenia podpisujúceho subjektu.

([1]) IETF, RFC 5652, syntax kryptografických správ (CMS), http://tools.ietf.org/html/rfc5652.
IETF, RFC 5035, zlepšené bezpečnostné služby (ESS). Aktualizácia: Pridanie agilnosti algoritmu CertID, http://tools.ietf.org/html/rfc5035.
IETF, RFC 3161, Internet X.509 Protokol časovej známky infraštruktúry verejného kľúča (TSP), http://tools.ietf.org/html/rfc3161.

([2]) ETSI TS 101 733 v.1.8.1: CMS zaručené elektronické podpisy (CAdES).

([3]) ETSI TS 102 176: elektronické podpisy a infraštruktúra (ESI); algoritmy a parametre pre bezpečné elektronické podpisy; časť 1: Funkcie Hash a asymetrické algoritmy; časť 2: „Bezpečné kanálové protokoly a algoritmy pre zariadenia na vytváranie podpisov".

([4]) Najnovšia verzia je D.SPA.13 ECRYPT2 Ročná správa o algoritmoch a kľúčových veľkostiach (2009 – 2010) z 30. marca 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabuľka 2

CAdES – BES (EPES)		**Spoločné minimálne požiadavky**
(ETSI TS 101 733 platí s nasledujúcimi profilovými prvkami)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
M = povinné; O = voliteľné; R = odporúčané; N = nepoužíva sa		
SignedData ::= SEQUENCE {		
version CMSVersion,		
DigestAlgorithms DigestAlgorithmIdentifiers,	M	**Algoritmy**: týkajú sa použiteľných vnútroštátnych právnych predpisov a na účely pokynov k správam ETSI TS 102 176 a ECRYPT2 D.SPA.7 pre ďalšie odporúčania.
encapContentInfo SEQUENCE {		
eContentType ContentType,	M	id-údaje
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	M/N	Podpísaný atribút ContentType je k dispozícii a obsahuje id-dáta (http://tools.ietf.org/html/rfc5652#section 4), kde typ obsahu dát má odkazovať na ľubovoľné oktetové rady ako UTF-8 text alebo objekt ZIP s podzložkou MimeType.
-- External data (if signature detached)*		Ak oddelený podpis nie je pripojený inak. * Externé dáta znamenajú údaje chránené oddeleným podpisom, ktorý nie je zahrnutý do CAdES podpisu eContent. Odporúča sa začleniť podpísané externé dáta spolu s podpisom v súbore ZIP.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	M	MUSÍ obsahovať osvedčenie X509 od autora podpisu. ODPORÚČA sa zaradiť osvedčenia z celého reťazca osvedčení až po „pevný bod“ dôvery.
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	O	
signerInfos SET	M	Najmenej jedna signerInfo.
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	O	(Nechránená hodnota)
digestAlgorithm DigestAlgorithmIdentifier,	M	**Algoritmy**: ďalšie odporúčania sa nachádzajú v platných vnútroštátnych právnych predpisoch a na účely pokynov v špecifikáciách ETSI TS 102 176 a správe ECRYPT2 D.SPA.7.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	M	
attrType OBJECT IDENTIFIER,	M/O	**POVINNÉ**: id-contentType (s údajmi id) id-messageDigest id-aa-ets-signingCertificateV2 alebo id-aa-signingCertificate POVINNÉ: signingTime **VOLITEĽNÉ**: id-aa-ets-sigPolicyId Ostatné voliteľné vlastnosti sú uvedené v ETSI TS 101 733.
attrValues SET AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmy**: ďalšie odporúčania sa nachádzajú v platných vnútroštátnych právnych predpisoch a na účely pokynov v špecifikáciách ETSI TS 102 176 a správe ECRYPT2 D.SPA.7.
signature OCTET STRING, -- SignatureValue		
signedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	O	

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

ODDIEL 3 – PAdES – ČASŤ 3 (BES/EPES)

Podpis MUSÍ obsahovať príponu podpisu PAdES-BES (alebo -EPES), ako sa uvádza v špecifikáciách ETSI TS 102778 PAdES – časť 3 ([1]), a MUSÍ vyhovovať všetkým týmto doplňujúcim špecifikáciám:

MD5 (RFC 1321) sa NESMIE použiť ako hašovací algoritmus. Ďalšie odporúčania týkajúce sa algoritmov a parametrov, ktoré sa vzťahujú na elektronické podpisy, môžu podpisujúce subjekty nájsť v platných vnútroštátnych predpisoch a na účely usmernení v technických špecifikáciách ETSI TS 102176 ([2]) a v správe ECRYPT2 D.SPA.x ([3]).

Podpísané atribúty MUSIA obsahovať odkaz na digitálne osvedčenia podpisujúceho subjektu X.509 v3 (RFC 5035) a pole *SignedData.certificates* (osvedčenia podpísaných údajov) MUSÍ obsahovať jeho hodnotu.

([1]) ETSI TS 102 778-3 v1.2.1: PDF zaručené elektronické podpisy (PAdES), PAdES zlepšené – PAdES – základné elektronické podpisy a PAdES – explicitná politika profilov elektronických podpisov.

([2]) ETSI TS 102 176: elektronické podpisy a infraštruktúra (ESI); algoritmy a parametre pre bezpečné elektronické podpisy; časť 1: Funkcie Hash a asymetrické algoritmy; časť 2: „Bezpečné kanálové protokoly a algoritmy pre zariadenia na vytváranie podpisov“.

([3]) Najnovšia verzia je D.SPA.13 ECRYPT2 Ročná správa o algoritmoch a kľúčových veľkostiach (2009 – 2010) z 30. marca 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Čas podpisu má podobu hodnoty zápisu **M** v adresári podpisov.

V prípade, že sa podpisy, ktoré používajú členské štáty, zakladajú na kvalifikovanom osvedčení, objekty PKI (reťazce osvedčení, revokačné údaje, časové známky), ktoré sú obsiahnuté v podpisoch, sa v súlade s rozhodnutím 2009/767/ES dajú overiť prostredníctvom zoznamu dôveryhodných informácií členského štátu, ktorý kontroluje alebo akredituje CSP na základe vystavenia osvedčenia podpisujúceho subjektu.