DECYZJE

DECYZJA KOMISJI

z dnia 25 lutego 2011 r.

w sprawie ustalenia minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie przez właściwe organy zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym

(notyfikowana jako dokument nr C(2011) 1081)

(Tekst mający znaczenie dla EOG)

(2011/130/UE)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotyczącą usług na rynku wewnętrznym [1], w szczególności jej art. 8 ust. 3,

a także mając na uwadze, co następuje:

(1) Usługodawcom, których usługi objęte są zakresem dyrektywy 2006/123/WE, należy zapewnić możliwość dopełnienia procedur i formalności koniecznych do podjęcia i prowadzenia działalności poprzez pojedyncze punkty kontaktowe i drogą elektroniczną. W granicach określonych w art. 5 ust. 3 dyrektywy 2006/123/WE, przy dopełnianiu takich procedur i formalności usługodawcy nadal mogą być w niektórych przypadkach zobowiązani do przedłożenia dokumentów w oryginale bądź w formie poświadczonej kopii lub poświadczonego tłumaczenia W takich przypadkach usługodawcy mogą być zobowiązani do przedłożenia dokumentów podpisanych elektronicznie przez właściwe organy.

(2) Decyzja Komisji 2009/767/WE z dnia 16 października 2009 r. ustanawiająca środki ułatwiające korzystanie z procedur realizowanych drogą elektroniczną poprzez „pojedyncze punkty kontaktowe" zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym [2] ułatwia transgraniczne posługiwanie się zaawansowanym podpisem elektronicznym weryfikowanym certyfikatem kwalifikowanym, między innymi zobowiązując państwa członkowskie do przeprowadzania oceny ryzyka przed nałożeniem na usługodawców obowiązku posługiwania się takim podpisem elektronicznym oraz określając zasady akceptacji przez państwa członkowskie zaawansowanych podpisów elektronicznych weryfikowanych certyfikatem kwalifikowanym i składanych za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego lub bez takiego urządzenia. Decyzja 2009/767/WE nie zajmuje się jednak kwestią formatu podpisu elektronicznego w wydawanych przez właściwe organy dokumentach, które usługodawcy muszą przedstawiać w ramach dopełniania odpowiednich procedur i formalności.

(3) Ponieważ obecnie właściwe organy korzystają z różnych formatów zaawansowanego podpisu elektronicznego w celu podpisywania wydawanych przez siebie dokumentów, państwo członkowskie otrzymujące taki dokument do przetworzenia może napotkać trudności techniczne ze względu na mnogość stosowanych formatów podpisu. Aby umożliwić usługodawcom transgraniczne dopełnienie obowiązujących ich procedur i formalności drogą elektroniczną, należy doprowadzić do sytuacji, w której państwa członkowskie posiadać będą techniczne możliwości obsługi co najmniej kilku formatów zaawansowanego podpisu elektronicznego, którym opatrzone są dokumenty przekazywane im przez właściwe organy innego państwa członkowskiego. Określenie pewnej liczby formatów zaawansowanego podpisu elektronicznego, które muszą być technicznie obsługiwane przez państwo członkowskie otrzymujące dokument, umożliwi większą automatyzację procedur elektronicznych i poprawi ich transgraniczną interoperacyjność.

(4) Państwa członkowskie, których właściwe organy korzystają z innych formatów podpisu elektronicznego niż powszechnie obsługiwane, mogły wdrożyć środki umożliwiające weryfikację ich podpisów również w innych państwach. W takim przypadku, aby umożliwić państwom członkowskim otrzymującym dokumenty poleganie na takich narzędziach weryfikacji, konieczne jest udostępnienie informacji o tych narzędziach w przystępny sposób, chyba że niezbędne informacje są już zawarte bezpośrednio w dokumentach elektronicznych, podpisach elektronicznych lub elektronicznych nośnikach dokumentów.

(5) Niniejsza decyzja nie ma wpływu na określenie przez państwa członkowskie, czym jest oryginał, poświadczona kopia lub poświadczone tłumaczenie. Jej celem jest wyłącznie ułatwienie weryfikacji podpisów elektronicznych używanych w oryginałach, poświadczonych kopiach lub poświadczonych tłumaczeniach, które usługodawcy mogą przedkładać za pośrednictwem pojedynczych punktów kontaktowych.

[1] Dz.U. L 376 z 27.12.2006, s. 36.
[2] Dz.U. L 274 z 20.10.2009, s. 36.

(6) Aby umożliwić państwom członkowskim wdrożenie niezbędnych narzędzi technicznych, niniejszą decyzję powinno stosować się od dnia 1 sierpnia 2011 r.

(7) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu ds. Dyrektywy o Usługach,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Format referencyjny podpisu elektronicznego

1. Państwa członkowskie wdrażają niezbędne środki techniczne umożliwiające im przetwarzanie elektronicznie podpisanych dokumentów przedkładanych przez usługodawców w ramach dopełniania procedur i formalności za pośrednictwem pojedynczych punktów kontaktowych, jak przewidziano w art. 8 dyrektywy 2006/123/WE, które to dokumenty są podpisane przez właściwe organy innych państw członkowskich zaawansowanym podpisem elektronicznym XML, CMS lub PDF w formacie BES lub EPES, zgodnym ze specyfikacją techniczną przedstawioną w załączniku.

2. Państwa członkowskie, których właściwe organy podpisują dokumenty, o których mowa w ust. 1, przy użyciu innych formatów podpisu elektronicznego niż formaty, o których mowa w tym samym ustępie, powiadamiają Komisję o istniejących możliwościach weryfikacji, za pomocą których pozostałe państwa członkowskie mogą weryfikować otrzymane podpisy elektroniczne w trybie *online*, nieodpłatnie i w sposób zrozumiały dla osób niebędących rodzimymi użytkownikami języka, chyba że niezbędne informacje są już zawarte w dokumencie, w podpisie elektronicznym lub w elektronicznym nośniku dokumentu. Komisja udostępnia te informacje wszystkim państwom członkowskim.

Artykuł 2

Stosowanie

Niniejszą decyzję stosuje się od dnia 1 sierpnia 2011 r.

Artykuł 3

Adresaci

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 25 lutego 2011 r.

W imieniu Komisji
Michel BARNIER
Członek Komisji

ZAŁĄCZNIK

Specyfikacje zaawansowanego podpisu elektronicznego XML, CMS lub PDF, które muszą być technicznie obsługiwane przez państwo członkowskie otrzymujące dokument

W niniejszej części dokumentu słowa kluczowe MUSI (MUST, SHALL), NIE MOŻNA (MUST NOT, SHALL NOT), WYMAGANY (REQUIRED), POWINIEN (SHOULD), NIE POWINIEN (SHOULD NOT), ZALECANY (RECOMMENDED), MOŻE (MAY) i FAKULTATYWNY (OPTIONAL) należy interpretować zgodnie z RFC 2119 ([1]).

SEKCJA 1 – XAdES-BES/EPES

Podpis jest zgodny ze specyfikacją podpisu XML opublikowaną przez W3C ([2]).

Podpis MUSI być przynajmniej w formie XAdES-BES (lub -EPES), zgodnej ze specyfikacją ETSI TS 101 903 ([3]), i zgodny ze wszystkimi wyszczególnionymi poniżej dodatkowymi specyfikacjami:

Element ds:CanonicalizationMethod, określający algorytm przekształcania na postać kanoniczną elementu SignedInfo przed dokonaniem obliczeń związanych z jego podpisaniem, może wskazywać tylko na jeden z następujących algorytmów:

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

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

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

Inne algorytmy ani niepomijające komentarzy wersje wyżej wymienionych algorytmów NIE POWINNY być stosowane do tworzenia podpisu, ale POWINNY być obsługiwane w celu zapewnienia możliwości weryfikacji podpisów stworzonych za ich pomocą.

Jako algorytmu funkcji skrótu NIE MOŻNA stosować MD5 (RFC 1321). Podpisujących odsyła się do obowiązujących przepisów krajowych, a na potrzeby wytycznych – do specyfikacji ETSI TS 102 176 ([4]) oraz do raportu ECRYPT2 D.SPA.x ([5]), gdzie można znaleźć dalsze zalecenia dotyczące algorytmów i parametrów, które mogą być stosowane w podpisach elektronicznych.

Stosowanie *przekształceń (transforms)* ograniczone jest do następujących:

Przekształcenia na postać kanoniczną: zob. odpowiednie specyfikacje powyżej;

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

Filtrowanie:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): ze względów kompatybilności i zgodności z XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): jako następca XPath ze względu na problemy z wydajnością

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

Przekształcenie XSLT (arkusz stylów).

Element ds:KeyInfo MUSI zawierać certyfikat X.509 v3 podpisującego (tzn. jego wartość, a nie tylko wskazanie na niego).

Podpisana właściwość podpisu „SigningCertificate" MUSI zawierać wartość skrótu (CertDigest) certyfikatu podpisującego zawartego w ds:KeyInfo oraz identyfikator wystawcy tego certyfikatu (IssuerSerial), natomiast NIE MOŻNA używać fakultatywnego URI w polu „SigningCertificate".

Podpisana właściwość podpisu „SigningTime" jest obecna i zawiera czas UTC wyrażony w postaci xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

Element DataObjectFormat MUSI być obecny i zawierać podelement MimeType.

W przypadku gdy stosowane przez państwa członkowskie podpisy elektroniczne weryfikowane są za pomocą certyfikatu kwalifikowanego, zawarte w podpisach obiekty infrastruktury klucza publicznego (łańcuchy certyfikatów, dane dotyczące unieważnienia, znaczniki czasu) są weryfikowane przy użyciu krajowej zaufanej listy publikowanej zgodnie z decyzją 2009/767/WE przez państwo członkowskie, które sprawuje nadzór nad podmiotem świadczącym usługi certyfikacyjne i będącym wystawcą certyfikatu podpisującego lub które udzieliło temu podmiotowi akredytacji.

Tabela 1 zawiera podsumowanie specyfikacji, które musi spełniać podpis XAdES-BES/EPES, aby był obsługiwany technicznie przez państwo członkowskie otrzymujące dokument.

([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]) Najnowsza wersja: D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), z dnia 30 marca 2010 r. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabela 1

XAdES–BES (EPES)		**Wspólne minimalne wymagania**
(Zastosowanie ma specyfikacja ETSI TS 103 903 z następującymi, profilowanymi elementami)		
O = obowiązkowy; F = fakultatywny; Z = zalecany; N = niewykorzystany		
ds: Signature ID	O	
ds: SignedInfo	O	
ds: CanonicalizationMethod	O	*Na potrzeby weryfikacji podpisu MUSZĄ być obsługiwane wszystkie wymienione poniżej algorytmy, natomiast tworzenie podpisu POWINNO BYĆ ograniczone do jednego z nich:* *— 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* *Inne metody ani niepomijające komentarzy („#WithComments") wersje wyżej wymienionych algorytmów NIE POWINNY być stosowane.*
ds: SignatureMethod	O	***Algorytmy:** zob. obowiązujące przepisy krajowe, a na potrzeby wytycznych – specyfikacje ETSI TS 102 176 oraz raport ECRYPT2 D.SPA.7, gdzie można znaleźć dalsze zalecenia.*
ds: Reference URI	O	Jedno wskazanie każdego oryginalnego obiektu danych, który ma zostać podpisany (URI może wskazywać także na obiekty zewnętrzne) + wskazanie na element SignedProperties.
ds: Transforms	F	*Aplikacje weryfikujące MUSZĄ obsługiwać wszystkie wymienione poniżej przekształcenia, natomiast aplikacja do tworzenia podpisu POWINNA ograniczać zastosowanie tych przekształceń do następujących:* *— Przekształcenia na postać kanoniczną: zob. powyżej* *— Kodowanie Base64* *— XPath i XPath Filter 2.0* *— Przekształcenie podpisu dołączonego* *— Przekształcenie XSLT*
ds: DigestMethod	O	***Algorytmy:** zob. obowiązujące przepisy krajowe, a na potrzeby wytycznych – specyfikacje ETSI TS 102 176 oraz raport ECRYPT2 D.SPA.x, gdzie można znaleźć dalsze zalecenia.*
ds: DigestValue	O	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	O	
ds: KeyInfo	O	MUSI zawierać certyfikat X.509 (podpisana właściwość „SigningCertificate" MUSI zawierać wartość skrótu certyfikatu podpisującego). ZALECANE jest, aby dla certyfikatu podpisującego przedstawić łańcuch certyfikacji jako podpowiedź ułatwiającą proces walidacji (w takim przypadku MUSI zostać przedstawiony certyfikat X.509).
ds: Object		
QualifyingProperties	O	
SignedProperties	O	O
SignedSignatureProperties	O	O
SigningTime	O	UTC (xsd: dateTime).
SigningCertificate	O	MUSI zawierać wartość skrótu certyfikatu podpisującego zawartego w ds:KeyInfo, natomiast pomija się fakultatywne URI (aplikacje MOGĄ poszukiwać lub znajdować certyfikat podpisującego w elemencie ds:KeyInfo na podstawie porównania odpowiednich skrótów).
SignaturePolicyIdentifier	F	tylko dla formy EPES (i wyższych form zbudowanych na podstawie EPES)
Signature ProductionPlace	F	
SignerRole	F	
/SignedSignatureProperties		
SignedDataObjectProperties	F	
DataObjectFormat	O	Jeśli pole to jest wykorzystane, aplikacje MUSZĄ zapewnić wyświetlanie obiektów danych użytkownikowi w odpowiednim formacie. Jeśli pole to jest wykorzystane, MUSI być użyty element potomny MimeType.
CommitmentTypeIndication	F	
AllDataObjectsTimeStamp	F	
IndividualDataObjectTimeStamp	F	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	F	
UnsignedSignatureProperties		
CounterSignature	F	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Topologia podpisu – sposób pakowania podpisanych oryginalnych plików i podpisów		
SignatureEnveloped		Wszystkie MUSZĄ być obsługiwane.
SignatureEnveloping		
SignatureDetached		

SEKCJA 2 – CAdES-BES/EPES:

Podpis jest zgodny ze specyfikacją podpisu CMS (Cryptographic Message Syntax) [1].

Podpis wykorzystuje atrybuty podpisu CAdES-BES (lub -EPES) określone w specyfikacji ETSI TS 101 733 [2] i jest zgodny z dodatkowymi specyfikacjami wyszczególnionymi w tabeli 2 poniżej.

Wszystkie atrybuty podpisu CAdES uwzględniane w obliczeniu skrótu znacznika czasu archiwizacji (ETSI TS 101 733 V1.8.1 Annex K) MUSZĄ być zakodowane w formacie DER, natomiast wszystkie pozostałe mogą być zakodowane w formacie BER w celu uproszczenia jednoprzebiegowego przetwarzania podpisu CAdES.

Jako algorytmu funkcji skrótu NIE MOŻNA stosować MD5 (RFC 1321). Podpisujących odsyła się do obowiązujących przepisów krajowych, a na potrzeby wytycznych – do specyfikacji ETSI TS 102 176 [3] oraz do raportu ECRYPT2 D.SPA.x [4], gdzie można znaleźć dalsze zalecenia dotyczące algorytmów i parametrów, które mogą być stosowane w podpisach elektronicznych.

Podpisane atrybuty MUSZĄ zawierać wskazanie na certyfikat X.509 v3 podpisującego (RFC 5035), a pole *SignedData.certificates* MUSI zawierać jego wartość.

Podpisany atrybut SigningTime MUSI być obecny i MUSI zawierać czas UTC wyrażony w postaci zgodnej z http://tools.ietf.org/html/rfc5652#section-11.3.

Podpisany atrybut ContentType MUSI być obecny i zawiera dane identyfikacyjne (http://tools.ietf.org/html/rfc5652#section-4), gdzie rodzaj zawartości danych ma wskazywać na dowolne ciągi oktetów, np. tekst UTF-8 lub kontener ZIP z podelementem MimeType.

W przypadku gdy stosowane przez państwa członkowskie podpisy elektroniczne weryfikowane są za pomocą certyfikatu kwalifikowanego, zawarte w podpisach obiekty infrastruktury klucza publicznego (łańcuchy certyfikatów, dane dotyczące unieważnienia, znaczniki czasu) są weryfikowane przy użyciu krajowej zaufanej listy publikowanej zgodnie z decyzją Komisji 2009/767/WE przez państwo członkowskie, które sprawuje nadzór nad podmiotem świadczącym usługi certyfikacyjne i będącym wystawcą certyfikatu podpisującego lub które udzieliło temu podmiotowi akredytacji.

---

[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] Najnowsza wersja: D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), z dnia 30 marca 2010 r. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabela 2

CAdES–BES (EPES)		**Wspólne minimalne wymagania**
(Zastosowanie ma specyfikacja ETSI TS 101 733 z następującymi, profilowanymi elementami)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
O = obowiązkowy; F = fakultatywny; Z = zalecany; N = niewykorzystany		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	**O**	**Algorytmy: zob. obowiązujące przepisy krajowe, a na potrzeby wytycznych – specyfikacje ETSI TS 102 176 oraz raport ECRYPT2 D.SPA.7, gdzie można znaleźć dalsze zalecenia.**
encapContentInfo SEQUENCE {	**O**	
eContentType ContentType,	**O**	**id-Data**
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	**O/N**	**Podpisany atrybut ContentType jest obecny i zawiera wartość id-Data (http://tools.ietf.org/html/rfc5652#section-4), gdzie rodzaj zawartości danych ma wskazywać na dowolne ciągi oktetów, np. tekst UTF-8 lub kontener ZIP z podelementem MimeType.**
-- External Data (if signature detached)*		**jeśli podpis jest oddzielony od podpisywanych danych; w przeciwnym razie wartość nie występuje * Dane zewnętrzne oznaczają zabezpieczone podpisem oddzielonym dane, które nie są zawarte w elemencie eContent podpisu CAdES. Podpisane dane zewnętrzne zaleca się umieszczać razem z podpisem w pliku ZIP.**
certificates [0] IMPLICIT CertificateSet OPTIONAL,	**O**	**MUSI zawierać certyfikat X.509 podpisującego. ZALECANE jest zamieszczenie certyfikatów z całego łańcucha certyfikacji aż do punktu zaufania.**
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	**F**	
signerInfos SET OF	**O**	**Co najmniej jedna wartość signerInfo.**
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	**F**	**(Wartość niezabezpieczona)**
digestAlgorithm DigestAlgorithmIdentifier,	**O**	**Algorytmy: zob. obowiązujące przepisy krajowe, a na potrzeby wytycznych – specyfikacje ETSI TS 102 176 oraz raport ECRYPT2 D.SPA.7, gdzie można znaleźć dalsze zalecenia.**
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	**O**	
attrType OBJECT IDENTIFIER,	**O/F**	**OBOWIĄZKOWE: id-contentType (wraz z danymi identyfikacyjnymi) id-messageDigest id-aa-ets-signingCertificateV2 lub id-aa-signingCertificate OBOWIĄZKOWY: signingTime FAKULTATYWNE: id-aa-ets-sigPolicyId Pozostałe atrybuty fakultatywne jak zdefiniowano w ETSI TS 101 733.**
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algorytmy: zob. obowiązujące przepisy krajowe, a na potrzeby wytycznych – specyfikacje ETSI TS 102 176 oraz raport ECRYPT2 D.SPA.7, gdzie można znaleźć dalsze zalecenia.**
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	**F**	

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

SEKCJA 3 – PAdES-PART 3 (BES/EPES):

Podpis MUSI korzystać z rozszerzenia PAdES-BES (lub -EPES), zgodnego ze specyfikacją PAdES-Part3 zawartą w dokumencie ETSI TS 102 778 ([1]), i być zgodny z wyszczególnionymi poniżej dodatkowymi specyfikacjami:

Jako algorytmu funkcji skrótu NIE MOŻNA stosować MD5 (RFC 1321). Podpisujących odsyła się do obowiązujących przepisów krajowych, a na potrzeby wytycznych – do specyfikacji ETSI TS 102 176 ([2]) oraz do raportu ECRYPT2 D.SPA.x ([3]), gdzie można znaleźć dalsze zalecenia dotyczące algorytmów i parametrów, które mogą być stosowane w podpisach elektronicznych;

Podpisane atrybuty MUSZĄ zawierać wskazanie na certyfikat X.509 v3 podpisującego (RFC 5035), a pole *SignedData.certificates* MUSI zawierać jego wartość;

([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]) Najnowsza wersja: D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), z dnia 30 marca 2010 r. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Czas podpisania jest podany jako wartość pozycji **M** w słowniku podpisu;

W przypadku gdy stosowane przez państwa członkowskie podpisy elektroniczne weryfikowane są za pomocą certyfikatu kwalifikowanego, zawarte w podpisach obiekty infrastruktury klucza publicznego (łańcuchy certyfikatów, dane dotyczące unieważnienia, znaczniki czasu) są weryfikowane przy użyciu krajowej zaufanej listy publikowanej zgodnie z decyzją 2009/767/WE przez państwo członkowskie, które sprawuje nadzór nad podmiotem świadczącym usługi certyfikacyjne i będącym wystawcą certyfikatu podpisującego lub które udzieliło temu podmiotowi akredytacji.