BESLUITEN

BESLUIT VAN DE COMMISSIE

van 25 februari 2011

tot vaststelling van minimumvoorschriften voor de grensoverschrijdende verwerking van documenten die door de bevoegde autoriteiten elektronisch zijn ondertekend krachtens Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt

(Kennisgeving geschied onder nummer C(2011) 1081)

(Voor de EER relevante tekst)

(2011/130/EU)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt [1], en met name artikel 8, lid 3,

Overwegende hetgeen volgt:

(1) Verrichters van diensten die onder Richtlijn 2006/123/EG vallen, moeten de voor de toegang tot en de uitoefening van hun activiteiten vereiste procedures en formaliteiten via de één-loketten en met elektronische middelen kunnen afwikkelen. Binnen de in artikel 5, lid 3, van Richtlijn 2006/123/EG vastgestelde grenzen kan het nog steeds het geval zijn dat de dienstverrichters originele documenten, voor eensluidend gewaarmerkte kopieën of authentieke vertalingen moeten indienen ter afwikkeling van dergelijke procedures en formaliteiten. In dergelijke gevallen kan het nodig zijn dat de dienstverrichters documenten indienen die digitaal door de bevoegde autoriteiten zijn ondertekend.

(2) Het grensoverschrijdende gebruik van geavanceerde elektronische handtekeningen die op een gekwalificeerd certificaat berusten is vergemakkelijkt door Beschikking 2009/767/EG van de Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het „één-loket" in het kader van Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt [2], waarbij de lidstaten er onder andere toe worden verplicht risicobeoordelingen uit te voeren alvorens deze elektronische handtekeningen verplicht te stellen voor dienstverrichters en waarbij regels worden vastgesteld voor de aanvaarding door de lidstaten van geavanceerde elektronische handtekeningen die op gekwalificeerde certificaten zijn gebaseerd en al dan niet met een veilig middel voor het aanmaken van handtekeningen zijn aangemaakt. Beschikking 2009/767/EG gaat echter niet in op de formaten voor elektronische handtekeningen in door de bevoegde autoriteiten afgegeven documenten die door de dienstverrichters ter afwikkeling van de desbetreffende procedures en formaliteiten moeten worden ingediend.

(3) Aangezien de bevoegde autoriteiten in de lidstaten momenteel verschillende formaten voor geavanceerde elektronische handtekeningen gebruiken om hun documenten elektronisch te ondertekenen, kunnen de ontvangende lidstaten die deze documenten moeten verwerken technische problemen ondervinden ten gevolge van de verscheidenheid aan gebruikte handtekeningformaten. Om dienstverrichters in staat te stellen met elektronische middelen hun procedures en formaliteiten grensoverschrijdend af te wikkelen, moet ervoor worden gezorgd dat ten minste enkele formaten voor geavanceerde elektronische handtekeningen door de lidstaten technisch kunnen worden ondersteund wanneer zij documenten ontvangen die door de bevoegde autoriteiten van andere lidstaten elektronisch zijn ondertekend. Het definiëren van een aantal door de ontvangende lidstaat technisch te ondersteunen formaten voor geavanceerde digitale handtekeningen maakt een grotere mate van automatisering mogelijk en bevordert de grensoverschrijdende interoperabiliteit van de elektronische procedures.

(4) De lidstaten waarvan de bevoegde autoriteiten andere dan de algemeen ondersteunde formaten voor digitale handtekeningen gebruiken, hebben mogelijk andere valideringswijzen ingevoerd met behulp waarvan hun handtekeningen ook grensoverschrijdend kunnen worden geverifieerd. Om ervoor te zorgen dat de ontvangende lidstaten op deze valideringsinstrumenten kunnen vertrouwen, moet in dergelijke gevallen informatie over deze instrumenten op een gemakkelijk toegankelijke wijze beschikbaar worden gesteld, tenzij de benodigde informatie al in de elektronische documenten, in de elektronische handtekeningen of in de elektronische documentdragers zelf is opgenomen.

(5) Dit besluit laat onverlet dat de lidstaten bepalen wat als een origineel, een voor eensluidend gewaarmerkte kopie of een authentieke vertaling wordt beschouwd. Het heeft slechts tot doel de verificatie van elektronische handtekeningen te vergemakkelijken waar deze worden gebruikt in de originelen, voor eensluidend gewaarmerkte kopieën of authentieke vertalingen die dienstverrichters mogelijk via de één-loketten moeten indienen.

[1] PB L 376 van 27.12.2006, blz. 36.
[2] PB L 274 van 20.10.2009, blz. 36.

(6) Teneinde de lidstaten in de gelegenheid te stellen de nodige technische instrumenten in te voeren, is het aangewezen dat dit besluit met ingang van 1 augustus 2011 van toepassing is.

(7) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het Comité dienstenrichtlijn,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Referentieformaat voor elektronische handtekeningen

1. De lidstaten brengen de nodige technische middelen tot stand om de elektronisch ondertekende documenten te kunnen verwerken die dienstverrichters ter afwikkeling van procedures en formaliteiten via de één-loketten indienen, zoals bepaald in artikel 8 van Richtlijn 2006/123/EG, en die door de bevoegde autoriteiten van andere lidstaten zijn ondertekend met een geavanceerde elektronische XML-, CMS- of PDF-handtekening in het BES- of EPES-formaat, die aan de technische specificaties in de bijlage voldoet.

2. De lidstaten waarvan de bevoegde autoriteiten de in de eerste alinea bedoelde documenten met andere dan de in die alinea bedoelde formaten voor digitale handtekeningen ondertekenen, stellen de Commissie op de hoogte van bestaande valideringsmogelijkheden waarmee andere lidstaten de ontvangen elektronische handtekeningen online, kosteloos en op een voor niet-moedertaalsprekers te begrijpen wijze kunnen valideren, tenzij de benodigde informatie al in het document of in de elektronische handtekening of elektronische documentdrager is opgenomen. De Commissie zal deze informatie beschikbaar stellen aan alle lidstaten.

Artikel 2

Toepassing

Dit besluit is van toepassing met ingang van 1 augustus 2011.

Artikel 3

Adressaten

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel, 25 februari 2011.

Voor de Commissie
Michel BARNIER
Lid van de Commissie

BIJLAGE

Specificaties voor een door de ontvangende lidstaat technisch te ondersteunen geavanceerde elektronische XML-, CMS- of PDF-handtekening

In het volgende onderdeel van dit document moeten de sleutelwoorden „MOETEN" (MUST, SHALL), „NIET MOGEN" (MUST NOT, SHALL NOT), „VERPLICHT" (REQUIRED), „ZOUDEN MOETEN" (SHOULD), „ZOUDEN NIET MOGEN" (SHOULD NOT), „AANBEVOLEN" (RECOMMENDED), „KUNNEN" (MAY) en „FACULTATIEF" (OPTIONAL) en daarvan afgeleide woordvormen worden uitgelegd zoals beschreven in RFC 2119 ([1]).

DEEL 1 — XAdES-BES/EPES

De handtekening voldoet aan de W3C-specificaties voor XML-handtekeningen ([2]).

De handtekening MOET ten minste een handtekening volgens de XAdES-BES- of XAdES-EPES-vorm zijn zoals gedefinieerd in de XAdES-specificaties ([3]) van ETSI TS 101 903; daarnaast voldoet zij aan de volgende aanvullende specificaties:

Het ds:CanonicalizationMethod-element, waarmee het algoritme voor omzetting in de canonieke vorm wordt gespecificeerd dat op het SignedInfo-element wordt toegepast alvorens de handtekeningberekeningen uit te voeren, verwijst slechts naar een van de volgende algoritmen:

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

Andere algoritmen of versies „met commentaar" van de bovengenoemde algoritmen ZOUDEN NIET MOGEN worden gebruikt voor het aanmaken van handtekeningen maar ZOUDEN wel MOETEN worden ondersteund met het oog op de achterwaartse interoperabiliteit van de handtekeningverificatie.

MD5 (RFC 1321) MAG NIET als hashingalgoritme worden gebruikt. De ondertekenaars worden verwezen naar de toepasselijke nationale wetgeving, en voor richtsnoeren naar ETSI TS 102 176 ([4]) en het ECRYPT2 D.SPA.x-verslag ([5]), voor verdere aanbevelingen inzake de geschikte algoritmen en parameters voor elektronische handtekeningen.

Het gebruik van transformaties (*transforms*) is beperkt tot de volgende lijst:

Transforms voor omzetting in de canonieke vorm: zie hierboven voor de bijbehorende specificaties;

Base64-codering (http://www.w3.org/2000/2009/xmldsig#base64);

Filtering

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): omwille van de compatibiliteit en de overeenstemming met XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/2006/xmldsig-filter2): als opvolger van XPath, in verband met prestatieproblemen;

Enveloped signature transform: (http://www.w3.org/2000/2009/xmldsig#enveloped-signature);

XSLT-transform (stylesheet-transformatie).

Het ds:KeyInfo-element MOET het digitale X.509 v3-certificaat van de ondertekenaar (d.w.z. de waarde ervan en niet slechts een verwijzing ernaar) bevatten.

De ondertekende eigenschap „SigningCertificate" van de handtekening MOET de hashwaarde (CertDigest) en de in ds:KeyInfo opgeslagen IssuerSerial van het certificaat van de ondertekenaar bevatten, en de facultatieve URI in het veld „SigningCertificate" MAG NIET worden gebruikt.

De ondertekende eigenschap SigningTime van de handtekening is aanwezig en bevat de UTC, uitgedrukt als xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

Het DataObjectFormat-element MOET aanwezig zijn en het MimeType-subelement bevatten.

Indien de door de lidstaten gebruikte handtekeningen op een gekwalificeerd certificaat zijn gebaseerd, kunnen de in de handtekeningen opgenomen PKI-objecten (certificaatketens, intrekkingsgegevens, tijdstempels) geverifieerd worden met behulp van de vertrouwenslijst, overeenkomstig Beschikking 2009/767/EG, van de lidstaat die toezicht houdt op of accreditatie verleent aan de certificatiedienstverlener die het certificaat van de ondertekenaar heeft afgegeven.

In tabel 1 zijn de specificaties samengevat waaraan een XAdES-BES/EPES-handtekening moet voldoen om door de ontvangende lidstaat technisch te worden ondersteund.

([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]) De recentste versie is D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010) van 30 maart 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabel 1

XAdES - BES (EPES)		**Gemeenschappelijke minimumvoorschriften**
(ETSI TS 103 903 is van toepassing met de volgende profielelementen)		
V=Verplicht; F=Facultatief; A=Aanbevolen; N=Niet gebruikt		
ds: Signature ID	V	
ds: SignedInfo	V	
ds: CanonicalizationMethod	V	*Alle hieronder genoemde algoritmen MOETEN worden ondersteund voor handtekeningverificatie, het aanmaken van handtekeningen ZOU tot een ervan beperkt MOETEN worden:* *- 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* *Andere methoden of "#WithComments"-versies van de bovengenoemde methoden ZOUDEN NIET MOGEN worden gebruikt.*
ds: SignatureMethod	V	***Algoritmen:*** *zie de toepasselijke nationale wetgeving en, voor richtsnoeren, ETSI TS 102 176 en het ECRYPT2 D.SPA.7-verslag voor verdere aanbevelingen.*
ds: Reference URI	V	Eén verwijzing naar ieder te ondertekenen gegevensobject (URI's kunnen ook naar een extern object wijzen), + verwijzing naar SignedProperties-element
ds: Transforms	F	*Verificatietoepassingen MOETEN alle hieronder genoemde transforms ondersteunen; in toepassingen voor het aanmaken van handtekeningen ZOU het gebruik van transforms tot de hieronder genoemde transforms MOETEN worden beperkt:* *- Transforms voor omzetting in de canonieke vorm: zie hierboven* *- Base64-codering* *- XPath en XPath Filter 2.0* *- Enveloped signature transform* *- XSLT-transforms*
ds: DigestMethod	V	***Algoritmen:*** *zie de toepasselijke nationale wetgeving en, voor richtsnoeren, ETSI TS 102 176 en het ECRYPT2 D.SPA.7-verslag voor verdere aanbevelingen.*
ds: DigestValue	V	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	V	
ds: KeyInfo	V	MOET X509-certificaat bevatten (de getekende eigenschap SigningCertificate MOET de hashwaarde van het certificaat van deze ondertekenaar bevatten) Het wordt AANBEVOLEN de certificatieketen van het certificaat van de ondertekenaar als aanwijzing beschikbaar te stellen om het validatieproces te vergemakkelijken (in dat geval MOETEN X.509-certificaten beschikbaar worden gesteld).
ds: Object		
QualifyingProperties	V	
SignedProperties	V	V
SignedSignatureProperties	V	V
SigningTime	V	UTC (xsd: dateTime).
SigningCertificate	V	MOET de hashwaarde van het certificaat van de ondertekenaar in ds:KeyInfo bevatten; de facultatieve URI blijft achterwege (toepassingen KUNNEN het certificaat van de ondertekenaar in ds:KeyInfo zoeken/vinden op basis van hashequivalentie).
SignaturePolicyIdentifier	F	alleen voor de EPES-vorm (en voor hogere vormen die op de EPES-vorm zijn gebaseerd)
Signature ProductionPlace	F	
SignerRole	F	
/SignedSignatureProperties		
SignedDataObjectProperties	F	
DataObjectFormat	V	Als dit veld wordt gebruikt, MOETEN toepassingen ervoor zorgen dat de gegevensobjecten dienovereenkomstig aan de gebruiker worden getoond. Als het wordt gebruikt, MOET een MimeType-dochterelement worden gebruikt.
CommitmentTypeIndication	F	
AllDataObjectsTimeStamp	F	
IndividualDataObjectTimeStamp	F	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	F	
UnsignedSignatureProperties		
CounterSignature	F	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Handtekeningtopologie - Inpakken van ondertekende originele bestanden en handtekeningen		
SignatureEnveloped		MOETEN alle worden ondersteund
SignatureEnveloping		
SignatureDetached		

DEEL 2 — CAdES-BES/EPES

De handtekening voldoet aan de specificaties voor CMS-handtekeningen (Cryptographic Message Syntax) ([1]).

De handtekening maakt gebruik van CAdES-BES- of CAdES-EPES-attributen zoals gedefinieerd in de CAdES-specificaties van ETSI TS 101 733 ([2]); daarnaast voldoet zij aan de aanvullende specificaties in tabel 2.

Alle attributen van CAdES die zijn opgenomen in de hashberekening van het tijdstempel van het archief (ETSI TS 101 733 V1.8.1, bijlage K) MOETEN DER-gecodeerd zijn; alle overige attributen kunnen BER-gecodeerd zijn om de one-passverwerking van CAdES te vergemakkelijken.

MD5 (RFC 1321) MAG NIET als hashingalgoritme worden gebruikt. De ondertekenaars worden verwezen naar de toepasselijke nationale wetgeving, en voor richtsnoeren naar ETSI TS 102 176 ([3]) en het ECRYPT2 D.SPA.x-verslag ([4]), voor verdere aanbevelingen inzake de geschikte algoritmen en parameters voor elektronische handtekeningen.

De ondertekende attributen MOETEN een verwijzing naar het digitale X.509 v3-certificaat (RFC 5035) van de ondertekenaar bevatten en het veld *SignedData.certificates* MOET de waarde daarvan bevatten.

Het ondertekende attribuut SigningTime MOET aanwezig zijn en MOET de UTC bevatten, uitgedrukt overeenkomstig http://tools.ietf.org/html/rfc5652#section-11.3.

Het ondertekende attribuut ContentType MOET aanwezig zijn en bevat id-data (http://tools.ietf.org/html/rfc5652#section-4), waarbij het type gegevensinhoud (*data content type*) bedoeld is om te verwijzen naar willekeurige octet-tekenreeksen, zoals tekst in UTF-8 of een ZIP-container met MimeType-subelement.

Indien de door de lidstaten gebruikte handtekeningen op een gekwalificeerd certificaat zijn gebaseerd, kunnen de in de handtekeningen opgenomen PKI-objecten (certificaatketens, intrekkingsgegevens, tijdstempels) geverifieerd worden met behulp van de vertrouwenslijst, overeenkomstig Beschikking 2009/767/EG, van de lidstaat die toezicht houdt op of accreditatie verleent aan de certificatiedienstverlener die het certificaat van de ondertekenaar heeft afgegeven.

([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]) De recentste versie is D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010) van 30 maart 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabel 2

CAdES - BES (EPES)		**Gemeenschappelijke minimumvoorschriften**
(ETSI TS 101.733 is van toepassing met de volgende profielelementen)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
V=Verplicht; F=Facultatief; A=Aanbevolen; N=Niet gebruikt		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	V	**Algoritmen**: zie de toepasselijke nationale wetgeving en, voor richtsnoeren, ETSI TS 102 176 en het ECRYPT2 D.SPA.7-verslag voor verdere aanbevelingen.
encapContentInfo SEQUENCE {		
eContentType ContentType,	V	id-Data
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	V/N	Het ondertekende attribuut ContentType is aanwezig en bevat id-data (http://tools.ietf.org/html/rfc5652#section-4), waarbij het type gegevensinhoud (data content type) bedoeld is om te verwijzen naar willekeurige octet-tekenreeksen, zoals tekst in UTF-8 of een ZIP-container met MimeType-subelement.
-- External Data (if signature detached)*		in het geval van een losse handtekening, anders niet aanwezig. * Onder "externe gegevens" worden gegevens verstaan die zijn beveiligd met een losse handtekening die niet in de eContent van de CAdES-handtekening is opgenomen. Het wordt aanbevolen ondertekende externe gegevens samen met de handtekening in een ZIP-bestand op te nemen.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	V	MOET X509-certificaat van de ondertekenaar bevatten. Het wordt AANBEVOLEN certificaten uit de hele certificatieketen tot aan een vertrouwensanker op te nemen.
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	F	
signerInfos SET OF	V	Ten minste één signerInfo
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	F	(Onbeveiligde waarde)
digestAlgorithm DigestAlgorithmIdentifier,	V	**Algoritmen**: zie de toepasselijke nationale wetgeving en, voor richtsnoeren, ETSI TS 102 176 en het ECRYPT2 D.SPA.7-verslag voor verdere aanbevelingen.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	V	
attrType OBJECT IDENTIFIER,	V/F	**VERPLICHT**: id-contentType (met id-data) id-messageDigest id-aa-ets-signingCertificateV2 of id-aa-signingCertificate VERPLICHT: signingTime **FACULTATIEF**: id-aa-ets-sigPolicyId Andere facultatieve attributen zoals gedefinieerd in ETSI TS 101 733.
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmen**: zie de toepasselijke nationale wetgeving en, voor richtsnoeren, ETSI TS 102 176 en het ECRYPT2 D.SPA.7-verslag voor verdere aanbevelingen.
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	F	
SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }	F	

DEEL 3 — PAdES-PART 3 (BES/EPES)

De handtekening MOET gebruikmaken van een PAdES-BES- of PAdES-EPES-handtekeningextensie zoals gedefinieerd in de PAdES-Part3-specificaties van ETSI TS 102 778 ([1]); daarnaast voldoet de handtekening aan de volgende aanvullende specificaties:

MD5 (RFC 1321) MAG NIET als hashingalgoritme worden gebruikt. De ondertekenaars worden verwezen naar de toepasselijke nationale wetgeving, en voor richtsnoeren naar ETSI TS 102 176 ([2]) en het ECRYPT2 D.SPA.x-verslag ([3]), voor verdere aanbevelingen inzake de geschikte algoritmen en parameters voor elektronische handtekeningen.

De ondertekende attributen MOETEN een verwijzing naar het digitale X.509 v3-certificaat (RFC 5035) van de ondertekenaar bevatten en het veld *SignedData.certificates* MOET de waarde daarvan bevatten.

([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]) De recentste versie is D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010) van 30 maart 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Het tijdstip van ondertekening wordt aangegeven door de waarde van de **M**-vermelding in het handtekeningwoordenboek.

Indien de door de lidstaten gebruikte handtekeningen op een gekwalificeerd certificaat zijn gebaseerd, kunnen de in de handtekeningen opgenomen PKI-objecten (certificaatketens, intrekkingsgegevens, tijdstempels) geverifieerd worden met behulp van de vertrouwenslijst, overeenkomstig Beschikking 2009/767/EG, van de lidstaat die toezicht houdt op of accreditatie verleent aan de certificatiedienstverlener die het certificaat van de ondertekenaar heeft afgegeven.