BESCHLÜSSE

BESCHLUSS DER KOMMISSION

vom 25. Februar 2011

über Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten, die gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt von zuständigen Behörden elektronisch signiert worden sind

(Bekannt gegeben unter Aktenzeichen K(2011) 1081)

(Text von Bedeutung für den EWR)

(2011/130/EU)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt [1], insbesondere auf Artikel 8 Absatz 3,

in Erwägung nachstehender Gründe:

(1) Dienstleistungserbringer, deren Dienstleistungen in den Anwendungsbereich der Richtlinie 2006/123/EG fallen, müssen die Möglichkeit haben, die zur Aufnahme oder Ausübung ihrer Dienstleistungstätigkeit notwendigen Verfahren und Formalitäten mit elektronischen Mitteln über die einheitlichen Ansprechpartner abzuwickeln. Innerhalb der durch Artikel 5 Absatz 3 der Richtlinie 2006/123/EG gesetzten Grenzen kann es dennoch vorkommen, dass von Dienstleistungserbringern zur Abwicklung solcher Verfahren und Formalitäten Originaldokumente, beglaubigte Kopien oder beglaubigte Übersetzungen verlangt werden. In solchen Fällen müssen die Dienstleistungserbringer möglicherweise Dokumente einreichen, die von zuständigen Behörden elektronisch signiert worden sind.

(2) Die grenzübergreifende Verwendung elektronischer Signaturen, die auf einem qualifizierten Zertifikat beruhen, wird durch die Entscheidung 2009/767/EG der Kommission vom 16. Oktober 2009 über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über „einheitliche Ansprechpartner" gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt [2] geregelt; die Mitgliedstaaten werden darin u.a. verpflichtet, Risikoabschätzungen durchzuführen, bevor sie von Dienstleistungserbringern diese elektronischen Signaturen verlangen, und es werden Regeln aufgestellt, nach denen die Mitgliedstaaten fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und mit oder ohne sichere Signaturerstellungseinheit erstellt wurden, anerkennen. Die Entscheidung 2009/767/EG regelt jedoch keine Formate für elektronische Signaturen in den von zuständigen Behörden ausgestellten Dokumenten, die von Dienstleistungserbringern zur Abwicklung solcher Verfahren und Formalitäten einzureichen sind.

(3) Die zuständigen Behörden in den Mitgliedstaaten verwenden gegenwärtig unterschiedliche Formate fortgeschrittener elektronischer Signaturen, um ihre Dokumente elektronisch zu signieren, so dass der empfangende Mitgliedstaat, der diese Dokumente verarbeiten muss, wegen der Vielfalt der verwendeten Signaturformate möglicherweise vor technische Probleme gestellt wird. Damit Dienstleistungserbringer ihre Verfahren und Formalitäten grenzübergreifend elektronisch abwickeln können, muss gewährleistet sein, dass die Mitgliedstaaten zumindest mehrere Formate fortgeschrittener elektronischer Signaturen technisch unterstützen, wenn sie Dokumente erhalten, die von zuständigen Behörden anderer Mitgliedstaaten elektronisch signiert worden sind. Die Festlegung mehrerer Formate fortgeschrittener elektronischer Signaturen, die der empfangene Mitgliedstaat technisch unterstützen muss, würde eine stärkere Automatisierung erlauben und die grenzübergreifende Interoperabilität elektronischer Verfahren verbessern.

(4) Mitgliedstaaten, deren zuständige Behörden andere als die gewöhnlich unterstützten Formate elektronischer Signaturen verwenden, haben möglicherweise Validierungsmittel vorgesehen, die auch grenzüberschreitend eine Überprüfung ihrer elektronischen Signaturen erlauben. Damit in diesem Fall der empfangende Mitgliedstaat auf diese Validierungswerkzeuge zurückgreifen kann, müssen Informationen über diese Werkzeuge in leicht zugänglicher Weise bereitgestellt werden, sofern die notwendigen Informationen nicht direkt in den elektronischen Dokumenten, in den elektronischen Signaturen oder in den Trägern der elektronischen Dokumente selbst enthalten sind.

(5) Dieser Beschluss lässt die Bestimmungen der Mitgliedstaaten in Bezug darauf, was ein Original, eine beglaubigte Kopie oder eine beglaubigte Übersetzung ist, unberührt. Sein Ziel beschränkt sich auf die Erleichterung der Überprüfung der elektronischen Signaturen, die in den Originalen, beglaubigten Kopien oder beglaubigten Übersetzungen verwendet werden, welche gegebenenfalls von Dienstleistungserbringern über die einheitlichen Ansprechpartner einzureichen sind.

[1] ABl. L 376 vom 27.12.2006, S. 36.
[2] ABl. L 274 vom 20.10.2009, S. 36.

(6) Damit die Mitgliedstaaten die notwendigen technischen Werkzeuge einrichten können, sollte dieser Beschluss ab dem 1. August 2011 gelten.

(7) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des für die Dienstleistungsrichtlinie eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Referenzformat für elektronische Signaturen

(1) Die Mitgliedstaaten schaffen die notwendigen technischen Mittel, die es ihnen erlauben, elektronisch signierte Dokumente zu verarbeiten, die von Dienstleistungserbringern im Rahmen der Abwicklung der Verfahren und Formalitäten über die einheitlichen Ansprechpartner gemäß Artikel 8 der Richtlinie 2006/123/EG eingereicht werden und die von zuständigen Behörden anderer Mitgliedstaaten entsprechend den im Anhang festgelegten technischen Spezifikationen mit einer fortgeschrittenen elektronischen XML-, CMS- oder PDF-Signatur im BES- oder EPES-Format signiert worden sind.

(2) Die Mitgliedstaaten, deren zuständige Behörden die in Absatz 1 genannten Dokumente mit elektronischen Signaturen in anderen als den im gleichen Absatz genannten Formaten signieren, teilen der Kommission die vorhandenen Validierungsmöglichkeiten mit, die es anderen Mitgliedstaaten erlauben, die empfangenen elektronischen Signaturen kostenlos und in einer für Nichtmuttersprachler verständlichen Weise online zu überprüfen, sofern die notwendigen Informationen nicht bereits in dem Dokument, der elektronischen Signatur oder dem Träger des elektronischen Dokuments enthalten ist. Die Kommission macht diese Informationen den Mitgliedstaaten zugänglich.

Artikel 2

Geltung

Dieser Beschluss gilt ab dem 1. August 2011.

Artikel 3

Adressaten

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 25. Februar 2011

Für die Kommission

Michel BARNIER

Mitglied der Kommission

ANHANG

Spezifikationen für eine fortgeschrittene elektronische Signatur (XML, CMS oder PDF), die durch den empfangenden Mitgliedstaat technisch unterstützt werden muss

Die im nachstehenden Teil dieses Dokuments verwendeten Schlüsselbegriffe „MUSS" bzw. „MÜSSEN", „DARF NICHT" bzw. „DÜRFEN NICHT", „ERFORDERLICH", „SOLLTE(N)", „SOLLTE(N) NICHT", „EMPFOHLEN", „KANN" bzw. „KÖNNEN" und „OPTIONAL" sind in Anlehnung an die in englischer Sprache in RFC 2119 ([1]) vorliegenden Begriffe auszulegen.

ABSCHNITT 1 — XAdES-BES/EPES

Die Signatur entspricht den Spezifikationen des W3C für die XML-Signatur ([2]).

Bei dem Format der Signatur MUSS es sich mindestens um XadES-BES (oder -EPES) gemäß den XAdES-Spezifikationen von ETSI TS 101 903 ([3]) handeln; sie entspricht den folgenden weiteren Spezifikationen:

Die „ds:CanonicalizationMethod", die den Kanonisierungsalgorithmus angibt, der vor dem Ausführen von Signaturberechnungen für das „SignedInfo"-Element verwendet wird, identifiziert nur einen der folgenden Algorithmen:

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

Andere Algorithmen oder Versionen „mit Kommentaren" der oben aufgeführten Algorithmen SOLLTEN NICHT für die Signaturerstellung verwendet werden, SOLLTEN aber in Bezug auf die verbleibende Interoperabilität für die Signaturüberprüfung unterstützt werden.

MD5 (RFC 1321) DARF NICHT als Digestalgorithmus verwendet werden. Signaturgeber werden auf geltende einzelstaatliche Rechtsvorschriften verwiesen und für Leitlinienzwecke auf ETSI TS 102 176 ([4]) sowie für weitere Empfehlungen zu Algorithmen und Parametern für elektronische Signaturen auf den ECRYPT2 D.SPA.x-Bericht ([5]).

Die Verwendung von *Transformationen* ist auf die nachfolgend beschriebenen beschränkt:

Kanonisierungstransformationen: siehe vorgenannte zugehörige Spezifikationen;

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

Filterung:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): aus Kompatibilitätsgründen und zur Übereinstimmung mit XMLDSig,

Xpath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): als Nachfolger für XPath aufgrund von Leistungsproblemen;

verschachtelte Signaturtransformation: (http://www.w3.org/2000/09/xmldsig#enveloped-signature);

XSLT-Transformation (Stylesheet).

Das „ds:KeyInfo"-Element MUSS das digitale X.509 v3-Zertifikat des Signaturgebers enthalten (d. h. dessen Wert, nicht nur einen Verweis darauf).

Die signierte Signatureigenschaft „SigningCertificate" MUSS den Digestwert („CertDigest") und den „IssuerSerial"-Verweis des im „ds:KeyInfo"-Element gespeicherten Zertifikats des Signaturgebers enthalten, und der optionale URI im Feld „SigningCertificate" DARF NICHT verwendet werden.

Die signierte Signatureigenschaft „SigningTime" ist vorhanden und enthält die UTC im Format „xsd:dateTime" („http://www.w3.org/TR/xmlschema-2/#dateTime").

Das „DataObjectFormat"-Element MUSS vorhanden SEIN und das Unterelement „MimeType" enthalten.

Wenn die von den Mitgliedstaaten verwendeten Signaturen auf einem qualifizierten Zertifikat beruhen, können die in den Signaturen enthaltenen PKI-Objekte (Zertifikatsketten, Sperrdaten, Zeitstempel) anhand der vertrauenswürdigen Liste des Mitgliedstaats, der den Zertifizierungsdiensteanbieter, von dem das Zertifikat ausgestellt wurde, beaufsichtigt bzw. akkreditiert hat, in Übereinstimmung mit der Entscheidung 2009/767/EG überprüft werden.

Tabelle 1 fasst die Spezifikationen zusammen, denen eine Signatur im Format XadES- BES/EPES entsprechen muss, um vom empfangenden Mitgliedstaat technisch unterstützt zu werden.

([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]) Bei der aktuellen Version handelt es sich um „D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010)" vom 30. März 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabelle 1

XAdES-BES (EPES)	**Allgemeine Mindestanforderungen**	
(ETSI TS 103 903 gilt mit den folgenden Profilelementen)		
V = Verbindlich; O = Optional; E = Empfohlen; N = Nicht verwendet		
ds: Signature ID	V	
ds: SignedInfo	V	
ds: CanonicalizationMethod	V	*Alle der folgenden Algorithmen MÜSSEN für die Signaturüberprüfung unterstützt werden, die Erstellung SOLLTE auf einen der folgenden beschränkt werden:* *— 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 oder Versionen „mit Kommentaren" der oben genannten Methoden SOLLTEN nicht verwendet werden.*
ds: SignatureMethod	V	***Algorithmen:*** *Verweis auf geltende einzelstaatliche Rechtsvorschriften und für Leitlinienzwecke auf ETSI TS 102 176 sowie für weitere Empfehlungen auf den ECRYPT2 D.SPA.7-Bericht.*
ds: Reference URI	V	Ein Verweis auf jedes zu signierende Originaldatenobjekt (URIs können auch auf externe Objekte verweisen) sowie ein Verweis auf das „SignedProperties"-Element
ds: Transforms	O	*Prüfanwendungungen MÜSSEN alle der folgenden Transformationen unterstützen; Anwendungen zur Signaturerstellung SOLLTEN die Verwendung dieser Transformationen auf die folgenden beschränken:* *— Kanonisierungstransformationen: siehe oben,* *— Base64-Codierung,* *— XPath und XPath Filter 2.0,* *— Verschachtelte Signaturtransformation,* *— XSLT-Transformationen.*
ds: DigestMethod	V	***Algorithmen:*** *Verweis auf geltende einzelstaatliche Rechtsvorschriften und für Leitlinienzwecke auf ETSI TS 102 176 sowie für weitere Empfehlungen auf den ECRYPT2 D.SPA.7-Bericht.*
ds: DigestValue	V	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	V	
ds: KeyInfo	V	MUSS das X.509-Zertifikat enthalten (Signatureigenschaft „SigningCertificate" MUSS den Digestwert des Zertifikats dieses Signaturgebers enthalten).
		Es wird EMPFOHLEN, die Zertifikatskette des Zertifikats des Signaturgebers als Hinweis für die Unterstützung des Überprüfungsprozesses vorzusehen (in diesem Fall MÜSSEN X.509-Zertifikate bereitgestellt werden).
ds: Object		
QualifyingProperties	V	
SignedProperties	V	V
SignedSignatureProperties	V	V
SigningTime	V	UTC („xsd:dateTime").
SigningCertificate	V	MUSS den Digestwert des Zertifikats des Signaturgebers in „ds:KeyInfo" enthalten; optionaler URI fällt weg (Anwendungen KÖNNEN basierend auf der Hashäquivalenz in „ds:KeyInfo" nach dem Zertifikat des Signaturgebers suchen/dieses finden).
SignaturePolicyIdentifier	O	nur für EPES-Format (und für übergeordnete Formate, die auf dem EPES-Format aufbauen)
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	V	Wenn dieses Feld verwendet wird, SOLLEN Anwendungen sicherstellen, dass Datenobjekte dem Benutzer entsprechend angezeigt werden. Bei Verwendung MUSS ein untergeordnetes „MimeType"-Element verwendet werden.
CommitmentTypeIndication	O	
AllDataObjectsTimeStamp	O	
IndividualDataObjectTimeStamp	O	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	O	
UnsignedSignatureProperties		
CounterSignature	O	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Signaturtopologie — Originaldateien mit Paketsignatur und Signaturen		
SignatureEnveloped		Alle MÜSSEN unterstützt werden.
SignatureEnveloping		
SignatureDetached		

ABSCHNITT 2 — CadES-BES/EPES

Die Signatur entspricht dem Syntaxstandard für kryptografische Mitteilungen (Cryptographic Message Syntax, CMS) für Signaturen ([1]).

Die Signatur verwendet CadES-BES-Signaturattribute (oder CadES-EPES-Signaturattribute) laut Definition in den CAdES-Spezifikationen von ETSI TS 101 733 ([2]) und entspricht ferner den in der nachfolgenden Tabelle 2 aufgeführten Spezifikationen.

Alle Attribute von CAdES, die in der Hashberechnung für Archivzeitstempel (ETSI TS 101 733 V1.8.1, Anhang K) enthalten sind, MÜSSEN DER-codiert sein; alle anderen können BER-codiert sein, um die Einwegverarbeitung von CAdES zu vereinfachen.

MD5 (RFC 1321) DARF NICHT als Digestalgorithmus verwendet werden. Signaturgeber werden auf geltende einzelstaatliche Rechtsvorschriften verwiesen und für Leitlinienzwecke auf ETSI TS 102 176 ([3]) sowie für weitere Empfehlungen zu Algorithmen und Parametern für elektronische Signaturen auf den ECRYPT2 D.SPA.x-Bericht ([4]).

Die signierten Attribute MÜSSEN einen Verweis auf das digitale X.509 v3-Zertifikat (RFC 5035) des Signaturgebers enthalten, und das Feld *SignedData.certificates* MUSS dessen Wert aufweisen.

Das signierte Attribut „SigningTime“ MUSS vorhanden sein und MUSS die UTC entsprechend der Definition unter „http://tools.ietf.org/html/rfc5652#section-11.3“ enthalten.

Das signierte Attribut „ContentType“ MUSS vorhanden sein und ID-Daten enthalten („http://tools.ietf.org/html/rfc5652#section-4“), wobei der Dateninhaltstyp auf beliebige Oktettzeichenfolgen verweist, z. B. UTF-8-Text oder ZIP-Container mit dem Unterelement „MimeType“.

Wenn die von den Mitgliedstaaten verwendeten Signaturen auf einem qualifizierten Zertifikat beruhen, können die in den Signaturen enthaltenen PKI-Objekte (Zertifikatsketten, Sperrdaten, Zeitstempel) anhand der vertrauenswürdigen Liste des Mitgliedstaats, der den Zertifizierungsdiensteanbieter, von dem das Zertifikat ausgestellt wurde, beaufsichtigt bzw. akkreditiert hat, in Übereinstimmung mit der Entscheidung 2009/767/EG überprüft werden.

([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]) Bei der aktuellen Version handelt es sich um „D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010)“ vom 30. März 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabelle 2

CAdES-BES (EPES)	**Allgemeine Mindestanforderungen**	
(ETSI TS 101 733 gilt mit den folgenden Profilelementen)		
ASN.1		
`ContentInfo ::= SEQUENCE {`		
`contentType ContentType, -- id-signedData`		
`content [0] EXPLICIT ANY DEFINED BY contentType }`		
	V = Verbindlich; O = Optional; E = Empfohlen; N = Nicht verwendet	
`SignedData ::= SEQUENCE {`		
`version CMSVersion,`		
`digestAlgorithms DigestAlgorithmIdentifiers,`	V	**Algorithmen:** Verweis auf geltende einzelstaatliche Rechtsvorschriften und für Leitlinienzwecke auf ETSI TS 102 176 sowie für weitere Empfehlungen auf den ECRYPT2 D.SPA.7-Bericht.
`encapContentInfo SEQUENCE {`		
`eContentType ContentType,`	V	ID-Daten
`eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },`	V/N	Das Signaturattribut „ContentType" ist vorhanden und enthält ID-Daten („http://tools.ietf.org/html/rfc5652#section-4"), wobei der Dateninhaltstyp auf beliebige Oktettzeichenfolgen verweist, z. B. UTF-8-Text oder ZIP-Container mit dem Unterelement „MimeType".
`--External Data (if signature detached *)`		sofern Signatur getrennt, andernfalls nicht vorhanden. *„Externe Daten" bedeutet, dass die Daten durch eine getrennte Signatur geschützt sind, die nicht im eContent der CAdES-Signatur enthalten ist. Es wird empfohlen, signierte externe Daten zusammen mit der Signatur in eine ZIP-Datei einzubinden.
`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	V	MUSS das X.509-Zertifikat des Signaturgebers enthalten. Die Einbindung von Zertifikaten aus der gesamten Zertifikatskette bis zu einem Vertrauensanker wird EMPFOHLEN.
`crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,`	O	
`signerInfos SET OF`	V	Mindestens eine Signaturgeberinformation
`SEQUENCE { -- SignerInfo`		
`version CMSVersion,`		
`sid SignerIdentifier,`	O	(Kein geschützter Wert)
`digestAlgorithm DigestAlgorithmIdentifier,`	V	**Algorithmen:** Verweis auf geltende einzelstaatliche Rechtsvorschriften und für Leitlinienzwecke auf ETSI TS 102 176 sowie für weitere Empfehlungen auf den ECRYPT2 D.SPA.7-Bericht.
`signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF`		
`SEQUENCE { -- Attribute`	V	
`attrType OBJECT IDENTIFIER,`	V/O	**MUSS:** „id-contentType" (mit ID-Daten) „id-messageDigest" „id-aa-ets-signingCertificateV2" oder „id-aa-signingCertificate" MUSS: „signingTime" **OPTIONAL:** „id-aa-ets-sigPolicyId"
		Weitere optionale Attribute laut Definition in ETSI TS 101 733.
`attrValues SET OF AttributeValue } OPTIONAL,`		
`signatureAlgorithm SignatureAlgorithmIdentifier,`		**Algorithmen:** Verweis auf geltende einzelstaatliche Rechtsvorschriften und für Leitlinienzwecke auf ETSI TS 102 176 sowie für weitere Empfehlungen auf den ECRYPT2 D.SPA.7-Bericht.
`signature OCTET STRING, -- SignatureValue`		
`unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF`	O	
`SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }`	O	

ABSCHNITT 3 — PAdES TEIL 3 (BES/EPES)

Die Signatur MUSS eine PAdES BES-Signaturerweiterung (oder PAdES EPES-Signaturerweiterung) gemäß PAdES Teil 3 (ETSI TS 102 778) [1] verwenden und den folgenden weiteren Spezifikationen entsprechen:

MD5 (RFC 1321) DARF NICHT als Digestalgorithmus verwendet werden. Signaturgeber werden auf geltende einzelstaatliche Rechtsvorschriften verwiesen und für Leitlinienzwecke auf ETSI TS 102 176 [2] sowie für weitere Empfehlungen zu Algorithmen und Parametern für elektronische Signaturen auf den ECRYPT2 D.SPA.x-Bericht [3].

Die signierten Attribute MÜSSEN einen Verweis auf das digitale X.509 v3-Zertifikat (RFC 5035) des Signaturgebers enthalten, und das Feld *SignedData.certificates* MUSS dessen Wert aufweisen.

[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] Bei der aktuellen Version handelt es sich um „D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010)" vom 30. März 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Der Signaturzeitpunkt wird durch den Wert des **M**-Eintrags im Signaturwörterbuch angegeben.

Wenn die von den Mitgliedstaaten verwendeten Signaturen auf einem qualifizierten Zertifikat beruhen, können die in den Signaturen enthaltenen PKI-Objekte (Zertifikatsketten, Sperrdaten, Zeitstempel) anhand der vertrauenswürdigen Liste des Mitgliedstaats, der den Zertifizierungsdiensteanbieter, von dem das Zertifikat ausgestellt wurde, beaufsichtigt bzw. akkreditiert hat, in Übereinstimmung mit der Entscheidung 2009/767/EG überprüft werden.