BESLUT

KOMMISSIONENS BESLUT

av den 25 februari 2011

om fastställande av minimikrav för behandling över gränserna av dokument som signerats elektroniskt av behöriga myndigheter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden

[delgivet med nr K(2011) 1081]

(Text av betydelse för EES)

(2011/130/EU)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden [1], särskilt artikel 8.3, och

av följande skäl:

(1) Tjänsteleverantörer vars tjänster omfattas av direktiv 2006/123/EG måste via gemensamma kontaktpunkter och på elektronisk väg kunna fullgöra förfaranden och formaliteter som krävs för tillträde till och utövande av deras verksamheter. Inom de gränser som fastställs i artikel 5.3 i direktiv 2006/123/EG kan det fortfarande finnas tillfällen då tjänsteleverantörer måste skicka originalhandlingar, bestyrkta kopior eller auktoriserade översättningar för att fullgöra förfaranden och formaliteter. Tjänsteleverantörerna kan då behöva skicka dokument som signerats elektroniskt av behöriga myndigheter.

(2) Gränsöverskridande användning av avancerade elektroniska signaturer som stöds av ett kvalificerat certifikat underlättas av kommissionens beslut 2009/767/EG av den 16 oktober 2009 om åtgärder som underlättar användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden [2], som bland annat ålägger medlemsstaterna att utföra riskbedömningar innan dessa elektroniska signaturer krävs från tjänsteleverantörer och fastställer regler för medlemsstaternas godkännande av avancerade elektroniska signaturer baserade på kvalificerade certifikat, med eller utan en säker anordning för skapande av signaturer. Beslut 2009/767/EG behandlar dock inte de elektroniska signaturernas format i dokument utfärdade av behöriga myndigheter som måste lämnas in av tjänsteleverantörer för att fullgöra relevanta förfaranden och formaliteter.

(3) Eftersom behöriga myndigheter i medlemsstaterna för närvarande använder avancerade elektroniska signaturer av olika format för att signera sina dokument elektroniskt kan de mottagande medlemsstaterna som måste behandla dokumenten ställas inför tekniska svårigheter till följd av den mångfald av signaturformat som används. För att möjliggöra för tjänsteleverantörer att fullgöra förfaranden och formaliteter över gränserna på elektronisk väg är det nödvändigt att se till att åtminstone ett visst antal format av avancerade elektroniska signaturer kan stödjas tekniskt av medlemsstaterna när de erhåller dokument som signerats elektroniskt av behöriga myndigheter i andra medlemsstater. Ett fastställande av ett antal format för avancerade elektroniska signaturer som måste stödjas tekniskt av den mottagande medlemsstaten skulle möjliggöra större automatisering och förbättra interoperabiliteten över gränserna.

(4) Medlemsstater vars behöriga myndigheter använder elektroniska signaturer av andra format än de som stöds normalt kan ha implementerat valideringsmetoder som gör det möjligt att verifiera deras signaturer även över gränserna. Om så är fallet och för att de mottagande medlemsstaterna ska kunna förlita sig på valideringsverktygen måste informationen om dessa verktyg göras tillgänglig på ett lättåtkomligt sätt, såvida inte den nödvändiga informationen inkluderas direkt i de elektroniska dokumenten, i de elektroniska signaturerna eller i de medier som innehåller de elektroniska dokumenten.

(5) Detta beslut påverkar inte medlemsstaternas fastställande av vad som utgör en originalhandling, en bestyrkt kopia eller en auktoriserad översättning. Syftet är endast att underlätta verifieringen av elektroniska signaturer om de används i originalhandlingar, bestyrkta kopior eller auktoriserade översättningar som tjänsteleverantörer måste lämna in via gemensamma kontaktpunkter.

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

(6) För att göra det möjligt för medlemsstaterna att implementera de nödvändiga tekniska verktygen bör beslutet tillämpas från och med den 1 augusti 2011.

(7) De åtgärder som föreskrivs i detta beslut är förenliga med tjänstedirektivkommitténs yttrande.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Referensformat för elektroniska signaturer

1. Medlemsstaterna ska tillämpa nödvändiga tekniska medel som gör det möjligt för dem att behandla elektroniskt signerade dokument som tjänsteleverantörer lämnar in i samband med fullgörandet av förfaranden och formaliteter via gemensamma kontaktpunkter, så som aviserades i artikel 8 i direktiv 2006/123/EG, och som signeras av behöriga myndigheter i andra medlemsstater med en avancerad elektronisk XML-, CMS- eller PDF-signatur i BES- eller EPES-format, som uppfyller de tekniska specifikationerna i bilagan.

2. Medlemsstater vars behöriga myndigheter signerar de dokument som omnämns i punkt 1 med hjälp av elektroniska signaturer i ett annat format än de som omnämns i samma punkt ska till kommissionen anmäla de existerande valideringsmöjligheterna så att andra medlemsstater ska kunna validera mottagna elektroniska signaturer på Internet, kostnadsfritt och på ett sätt som är begripligt för personer med ett annat modersmål, såvida inte den nödvändiga informationen redan finns i dokumentet, i den elektroniska signaturen eller i de medier som innehåller de elektroniska dokumenten. Kommissionen gör den informationen tillgänglig för alla medlemsstater.

Artikel 2

Tillämpning

Detta beslut ska tillämpas från och med den 1 augusti 2011.

Artikel 3

Adresser

Detta beslut riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 25 februari 2011.

På kommissionens vägnar

Michel BARNIER

Ledamot av kommissionen

BILAGA

Specifikationer för att en avancerad elektronisk XML-, CMS- eller PDF-signatur ska kunna stödjas tekniskt av den mottagande medlemsstaten

Nyckelorden MÅSTE, FÅR INTE, OBLIGATORISK, SKA, SKA INTE, BÖR, BÖR INTE, REKOMMENDERAD, FÅR och VALFRI ska i den nedanstående delen av dokumentet tolkas i enlighet med RFV 2119 ([1]).

AVSNITT 1 – XAdES-BES/EPES

Signaturens format ska följa W3C:s specifikationer för XML-signaturer ([2])

Signaturen MÅSTE ha signaturformatet XAdES-BES (eller -EPES) i enlighet med specifikationerna för XAdES i Etsi TS 101 903 ([3]) och även uppfylla samtliga nedanstående specifikationer:

Den ds:CanonicalizationMethod som specificerar den kanoniseringsalgoritm som tillämpas på SignedInfo-elementet innan signaturberäkning utförs identifierar endast en av följande algoritmer:

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

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

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

Andra algoritmer eller versioner ”med kommentarer” av ovan nämnda algoritmer BÖR INTE användas för att skapa signaturer, men BÖR stödjas för fortsatt interoperabilitet vid signaturverifieringen.

MD5 (RFC 1321) FÅR INTE användas som en digest algorithm. Undertecknare hänvisas till gällande nationell lagstiftning, och för riktlinjer till Etsi TS 102 176 ([4]) och till rapporten ECRYPT2 D.SpA.x ([5]) för ytterligare rekommendationer om algoritmer och parametrar som är möjliga för elektroniska signaturer.

Användningen av *transforms* begränsas till nedanstående lista:

Kanoniseringstransformer: se relaterade specifikationer ovan.

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

Filtrering:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): av kompatibilitetsskäl och för överensstämmelse med XMLDSig.

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): som en efterföljare till XPath på grund av prestanda-problem.

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

XSLT (stilmall) **transformer**.

ds:KeyInfo-elementet MÅSTE inkludera undertecknarens digitala X.509 v3-certifikat (dvs. dess värde och inte en referens till det).

Signaturegenskapen signerad med ”SigningCertificate” MÅSTE innehålla checksumman (CertDigest) och IssuerSerial för undertecknarens certifikat som lagras i ds:KeyInfo och det valfria URI i fältet ”SigningCertificate” FÅR INTE användas.

SigningTime för den signerade signaturegenskapen finns och innehåller UTC uttryckt som xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

DataObjectFormat-elementet MÅSTE finnas och innehålla MimeType-underelementet.

Om de signaturer som medlemsstaterna använder baseras på ett kvalificerat certifikat kan de PKI-objekt (certifikatkedjor, återkallningsdata, tidsstämplar) som ingår i signaturerna verifieras med hjälp av den tillförlitliga förteckningen, i enlighet med kommissionens beslut 2009/767/EG, av den medlemsstat som övervakar eller ackrediterar den CSP som utfärdat undertecknarens certifikat.

I tabell 1 sammanfattas de specifikationer som en XAdES-BES/EPES-signatur måste uppfylla för att stödjas tekniskt av den mottagande medlemsstaten.

([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; del 1: Hash functions and asymmetric algorithms; del 2: ”Secure channel protocols and algorithms for signature creation devices”.
([5]) Senaste versionen är D.SpA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), av den 30 mars 2010 (http://www.ecrypt.eu.org/documents/D.SpA.13.pdf).

Tabell 1

XAdES - BES (EPES)		**Gemensamma minimikrav**
(ETSI TS 103 903 gäller med följande profilelement)		
O=Obligatoriskt; V=Valfritt; R=Rekommenderat; A=Används inte		
ds: Signature Id	O	
ds: SignedInfo	O	
ds: CanonicalizationMethod	O	*Samtliga nedanstående algoritmer MÅSTE stödjas för signaturverifiering, för skapande BÖR de begränsas till en av följande:* *- 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* *Andra metoder eller versioner "#Med kommentarer" av ovanstående versioner BÖR INTE användas.*
ds: SignatureMethod	O	***Algoritmer:*** *se gällande nationell lagstiftning och för riktlinjer ETSI TS 102 176 och rapporten ECRYPT2 D.SPA.7 för ytterligare rekommendationer.*
ds: Reference URI	O	En referens till varje ursprungsdataobjekt som ska signeras (URI:er kan även peka på externa objekt), + referens till SignedProperties-element
ds: Transforms	V	*Verifieringsapplikationer MÅSTE stödja alla nedanstående transformer medan applikationer för att skapa signaturer BÖR begränsas till endast en av transformerna nedan:* *– Kanoniseringstransformer: se ovan* *– Base64-kodning* *– XPath och XPath Filter 2.0* *– Enveloped signature-transform* *– XSLT-transformer*
ds: DigestMethod	O	***Algoritmer:*** *se gällande nationell lagstiftning och för riktlinjer ETSI TS 102 176 och rapporten ECRYPT2 D.SPA.7 för ytterligare rekommendationer.*
ds: DigestValue	O	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	O	
ds: KeyInfo	O	MÅSTE innehålla X509-certifikat (signeringsegenskapen SigningCertificate MÅSTE innehålla digestvärdet från undertecknarens certifikat) Det REKOMMENDERAS att certifieringskedjan för undertecknarens certifikat tillhandahålls för att underlätta valideringsprocessen (X.509-certifikat MÅSTE i så fall tillhandahållas).
ds: Object		
QualifyingProperties	O	
SignedProperties	O	O
SignedSignatureProperties	O	O
SigningTime	O	UTC (xsd: dateTime).
SigningCertificate	O	MÅSTE innehålla digestvärdet för undertecknarens certifikat som finns lagrat i ds:KeyInfo och valfritt URI utesluts (Appliaktioner KAN söka efter/leta upp undertecknarens certifikat i ds:KeyInfor baserat på hashekvivalens).
SignaturePolicyIdentifier	V	endast för EPES-format (och för högre format som baseras på EPES-formatet)
Signature ProductionPlace	V	
SignerRole	V	
/SignedSignatureProperties		
SignedDataObjectProperties	V	
DataObjectFormat	O	När det här fältet används SKA applikationer säkerställa att dataobjekt visas på samma sätt för användaren. När det används MÅSTE ett underordnat MimeType-element användas.
CommitmentTypeIndication	V	
AllDataObjectsTimeStamp	V	
IndividualDataObjectTimeStamp	V	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	V	
UnsignedSignatureProperties		
CounterSignature	V	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Signaturtopologi – förpacka signerade originalfiler och signaturer		
SignatureEnveloped		Alla MÅSTE stödjas
SignatureEnveloping		
SignatureDetached		

AVSNITT 2 – CAdES-BES/EPES

Signaturen överensstämmer med specifikationerna för CMS-signatur (Cryptographic Message Syntax) [1]

Signaturen använder de signaturattribut för CAdES-BES (eller -EPES) som specificeras i CAdES-specifikationerna i Etsi TS 101 733 [2] och uppfyller de övriga specifikationerna i tabell 2.

Alla CAdES-attribut som ingår i hashberäkningen av tidsstämpeln i arkivet (Etsi TS 101 733 V1.8.1 Annex K) MÅSTE vara DER-kodade och övriga kan vara i BER för att förenkla enstegsbearbetning av CAdES.

MD5 (RFC 1321) FÅR INTE användas som en digest algorithm. Undertecknare hänvisas till gällande nationell lagstiftning, och för riktlinjer till Etsi TS 102 176 [3] och till rapporten ECRYPT2 D.SpA.x [4] för ytterligare rekommendationer om algoritmer och parametrar som är möjliga för elektroniska signaturer.

De undertecknade attributen MÅSTE inkludera en referens till undertecknarens digitala X.509 v3-certifikat (RFC 5035) och fältet *SignedData.certificates* MÅSTE inkludera dess värde.

Signeringsattributet SigningTime MÅSTE finnas och MÅSTE innehålla UTC uttryckt som i http://tools.ietf.org/html/rfc5652#section-11.3.

Signeringsattributet ContentType MÅSTE finnas och innehålla id-data (http://tools.ietf.org/html/rfc5652#section-4) där datainnehållstypen är avsedd att hänvisa till arbiträra oktettsträngar, t.ex. UTF-8-text eller zip-container med MimeType-underelement.

Om de signaturer som medlemsstaterna använder baseras på ett kvalificerat certifikat kan de PKI-objekt (certifikatkedjor, återkallningsdata, tidsstämplar) som ingår i signaturerna verifieras med hjälp av den tillförlitliga förteckningen, i enlighet med beslut 2009/767/EG, av den medlemsstat som övervakar eller ackrediterar den CSP som utfärdat undertecknarens certifikat.

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

[4] Senaste versionen är D.SpA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), av den 30 mars 2010 (http://www.ecrypt.eu.org/documents/D.SpA.13.pdf).

Tabell 2

CAdES - BES (EPES)		Gemensamma minimikrav
(ETSI TS 101 733 gäller med följande profilelement)		
ASN.1		
`ContentInfo ::= SEQUENCE {`		
`contentType ContentType, -- id-signedData`		
`content [0] EXPLICIT ANY DEFINED BY contentType }`		
O=Obligatoriskt; V=Valfritt; R=Rekommenderat; A=Används inte		
`SignedData ::= SEQUENCE {`		
`version CMSVersion,`		
`digestAlgorithms DigestAlgorithmIdentifiers,`	O	**Algoritmer**: se gällande nationell lagstiftning och för riktlinjer ETSI TS 102 176 och rapporten ECRYPT2 D.SPA.7 för ytterligare rekommendationer.
`encapContentInfo SEQUENCE {`		
`eContentType ContentType,`	O	id-Data
`eContent [0] EXPLICIT OCTET STRING OPTIONAL -- finns inte om signaturen är separat },`	O/A	Signeringsattributet ContentType finns och innehåller id-data (http://tools.ietf.org/html/rfc5652#section-4) där datainnehållstypen är avsedd att hänvisa till arbiträra oktettsträngar, t.ex. UTF-8-text eller zip-container med MimeType-underelement.
`-- Externa data (om signaturen är separat)*`		Om en separat signatur inte finns på annan plats. * Externa data innebär data som är skyddade av en separat signatur som inte ingår i eContent för CAdES-signaturen. Det rekommenderas att undertecknade externa data inkluderas tillsammans med signaturen i zip-filen.
`certificat[0] IMPLICIT CertificateSet VALFRITT,`	O	MÅSTE innehålla X509-certifikat från undertecknaren. Det REKOMMENDERAS att certifikat från hela certifieringskedjan till och med ett tillitsankare inkluderas.
`crls [1] IMPLICIT RevocationInfoChoices VALFRITT,`	V	
`signerInfos SET OF`	O	Minst en signerInfo
`SEQUENCE { -- SignerInfo`		
`version CMSVersion,`		
`sid SignerIdentifier,`	V	(Inte skyddat värde)
`digestAlgorithm DigestAlgorithmIdentifier,`	O	**Algoritmer**: se gällande nationell lagstiftning och för riktlinjer ETSI TS 102 176 och rapporten ECRYPT2 D.SPA.7 för ytterligare rekommendationer.
`signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF`		
`SEQUENCE { -- Attribute`	O	
`attrType OBJECT IDENTIFIER,`	O/V	**MÅSTE**: id-contentType (med id-data) id-messageDigest id-aa-ets-signingCertificateV2 eller id-aa-signingCertificate MÅSTE: signingTime **VALFRITT**: id-aa-ets-sigPolicyId Andra valfria attribut enligt definitionen i ETSI TS 101 733.
`attrValues SET OF AttributeValue } VALFRITT,`		
`signatureAlgorithm SignatureAlgorithmIdentifier,`		**Algoritmer**: se gällande nationell lagstiftning och för riktlinjer ETSI TS 102 176 och rapporten ECRYPT2 D.SPA.7 för ytterligare rekommendationer.
`signature OCTET STRING, -- SignatureValue`		
`unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF`	V	
`SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } VALFRITT } } }`	V	

AVSNITT 3 – PAdES-PART 3 (BES/EPES)

Signaturen MÅSTE ha signaturformatet PAdES-BES (eller -EPES) i enlighet med specifikationerna för PAdES-Part3 i Etsi TS 102 778 ([1]) och även uppfylla samtliga nedanstående specifikationer:

MD5 (RFC 1321) FÅR INTE användas som en digest algorithm. Undertecknare hänvisas till gällande nationell lagstiftning, och för riktlinjer till Etsi TS 102 176 ([2]) och till rapporten ECRYPT2 D.SpA.x ([3]) för ytterligare rekommendationer om algoritmer och parametrar som är möjliga för elektroniska signaturer.

De undertecknade attributen MÅSTE inkludera en referens till undertecknarens digitala X.509 v3-certifikat (RFC 5035) och fältet *SignedData.certificates* MÅSTE inkludera dess värde.

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

([3]) Senaste versionen är D.SpA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), av den 30 mars 2010 (http://www.ecrypt.eu.org/documents/D.SpA.13.pdf).

Tiden för undertecknandet anges genom värdet på **M**-registreringen i signaturkatalogen.

Om de signaturer som medlemsstaterna använder baseras på ett kvalificerat certifikat kan de PKI-objekt (certifikatkedjor, återkallningsdata, tidsstämplar) som ingår i signaturerna verifieras med hjälp av den tillförlitliga förteckningen, i enlighet med beslut 2009/767/EG, av den medlemsstat som övervakar eller ackrediterar den CSP som utfärdat undertecknarens certifikat.