# AFGØRELSER

## KOMMISSIONENS AFGØRELSE

**af 25. februar 2011**

**om fastsættelse af mindstekrav ved behandling af elektronisk underskrevne dokumenter på tværs af grænserne foretaget af de kompetente myndigheder som omhandlet i Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked**

*(meddelt under nummer K(2011) 1081)*

**(EØS-relevant tekst)**

(2011/130/EU)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets direktiv 2006/123/EF af 12. december 2006 om tjenesteydelser i det indre marked [1], særlig artikel 8, stk. 3, og

ud fra følgende betragtninger:

(1) Tjenesteydere, hvis tjenester falder ind under direktiv 2006/123/EF, skal gennem kvikskranker og ved hjælp af elektroniske midler kunne gennemføre de procedurer og formaliteter, der er nødvendige for at få adgang til og for at udføre deres aktiviteter. Inden for de grænser, der er fastlagt i artikel 5, stk. 3, i direktiv 2006/123/EF, kan der stadig være tilfælde, hvor tjenesteydere skal fremsende originale dokumenter, bekræftede kopier eller bekræftede oversættelser for at gennemføre sådanne procedurer og formaliteter. I sådanne tilfælde kan det være nødvendigt for tjenesteydere at fremsende dokumenter, der er underskrevet elektronisk af kompetente myndigheder.

(2) Anvendelsen af avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat, på tværs af grænserne fremmes ved Kommissionens beslutning 2009/767/EF af 16. oktober 2009 om fastlæggelse af foranstaltninger, der skal lette anvendelsen elektroniske procedurer ved hjælp af »kvikskranker« i henhold til Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked [2], som bl.a. pålægger medlemsstaterne at foretage risikoanalyser, før de kræver disse elektroniske signaturer fra tjenesteydere, og fastlægger regler for medlemsstaternes accept af avancerede elektroniske signaturer, der er baseret på kvalificerede certifikater med eller uden et sikkert signaturgenereringssystem. Beslutning 2009/767/EF omhandler dog ikke formater for elektroniske signaturer i dokumenter udstedt af kompetente myndigheder, som skal fremsendes af tjenesteydere, når de gennemfører de relevante procedurer og formaliteter.

(3) Da de kompetente myndigheder i medlemsstaterne i øjeblikket anvender forskellige formater af avancerede elektroniske signaturer til at underskrive deres dokumenter elektronisk, kan de medlemsstater, der skal behandle disse dokumenter, have tekniske problemer som følge af de forskellige signaturformater, der anvendes. For at gøre det muligt for tjenesteydere at gennemføre deres procedurer og formaliteter elektronisk på tværs af grænserne er det nødvendigt at sikre, at i det mindste en række af avancerede formater for elektroniske signaturer kan understøttes teknisk af medlemsstaterne, når de modtager elektronisk underskrevne dokumenter fra de kompetente myndigheder i andre medlemsstater. Ved at fastlægge en række formater for avancerede elektroniske signaturer, som den modtagende medlemsstat skal understøtte teknisk, kan man give mulighed for en større grad af automatisering og forbedre elektroniske procedurers interoperabilitet på tværs af grænserne.

(4) Medlemsstater, hvis kompetente myndigheder anvender andre formater for elektroniske signaturer end dem, der normalt understøttes, kan have implementeret valideringsmetoder, der gør det muligt at validere deres signaturer også på tværs af grænserne. Når dette er tilfældet, og for at sætte den modtagende medlemsstat i stand til at stole på disse valideringsværktøjer, er det nødvendigt at give adgang til information om disse værktøjer på en let tilgængelig måde, medmindre de nødvendige oplysninger indgår direkte i de elektroniske dokumenter, i de elektroniske signaturer eller i de elektroniske »konvolutter«, som de elektroniske dokumenter fremsendes med.

(5) Denne afgørelse berører ikke medlemsstaternes bestemmelse af, hvad der udgør en original, en bekræftet kopi eller en bekræftet oversættelse. Dens mål er begrænset til at lette kontrollen af elektroniske signaturer, hvis de bruges i originaler, bekræftede kopier eller bekræftede oversættelser, som det kan være nødvendigt for tjenesteyderne at fremsende via kvikskrankerne.

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

(6) For at gøre det muligt for medlemsstaterne at implementere de nødvendige tekniske værktøjer vil det være hensigtsmæssigt, at denne afgørelse finder anvendelse fra den 1. august 2011.

(7) De i denne afgørelse fastsatte foranstaltninger er i overensstemmelse med udtalelse fra Udvalget for Tjenesteydelsesdirektivet —

VEDTAGET DENNE AFGØRELSE

*Artikel 1*

**Referenceformat for elektroniske signaturer**

1. Medlemsstaterne tilvejebringer de nødvendige tekniske midler til at sætte dem i stand til at behandle elektronisk underskrevne dokumenter, som tjenesteydere fremsender via kvikskrankerne for at gennemføre procedurer og formaliteter i henhold til artikel 8 i direktiv 2006/123/EF, og som er underskrevet af kompetente myndigheder i en anden medlemsstat med en avanceret elektronisk XML-, CMS- eller PDF-signatur i BES- eller EPES-format, som er i overensstemmelse med de tekniske specifikationer i bilaget.

2. Medlemsstater, hvis kompetente myndigheder underskriver de i stk. 1 omhandlede dokumenter med andre formater for elektroniske signaturer end de i samme afsnit omhandlede, skal meddele Kommissionen eksisterende valideringsmuligheder, som gør det muligt for andre medlemsstater gratis at validere de modtagne elektroniske signaturer online på en sådan måde, at det er forståeligt for ikke indfødte sprogbrugere, medmindre de påkrævede oplysninger allerede indgår i dokumentet, den elektroniske signatur eller den elektroniske »konvolut«, som dokumentet fremsendes med. Kommissionen stiller sådanne oplysninger til rådighed for alle medlemsstaterne.

*Artikel 2*

**Anvendelse**

Denne afgørelse anvendes fra den 1. august 2011.

*Artikel 3*

**Adressater**

Denne afgørelse er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 25. februar 2011.

*På Kommissionens vegne*

Michel BARNIER

*Medlem af Kommissionen*

*BILAG*

**Specifikationer for en XML, CMS eller PDF avanceret elektronisk signatur, der skal understøttes teknisk af den modtagende medlemsstat**

I den følgende del af dokumentet skal nøgleordene »SKAL«, »KRÆVES«, »SKAL«, »MÅ IKKE«, »BØR«, »BØR IKKE«, »ANBEFALET«, »KAN« og »VALGFRI« tolkes som beskrevet i RFC 2119 ([1]).

SEKTION 1 — XAdES-BES/EPES

Signaturen er i overensstemmelse med W3C XML-signaturspecifikationerne ([2]).

Signaturen SKAL mindst være en XAdES-BES-signaturformular (eller -EPES-signaturformular) som specificeret i XadES-specifikationerne ([3]) og i overensstemmelse med følgende supplerende specifikationer:

Metoden ds:CanonicalizationMethod, der specificerer den kanonikaliseringsalgoritme, der er anvendt på SignedInfo-elementet før udførelse af signaturberegninger, identificerer kun en af følgende algoritmer:

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

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

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

Andre algoritmer eller versioner af ovenstående algoritmer »med kommentarer« BØR IKKE anvendes til signaturgenereringen men BØR understøttes med henblik på residuel interoperabilitet ved signaturkontrol.

MD5 (RFC 1321) MÅ IKKE bruges som en digest-algoritme. Underskrivere henvises til gældende nationale love og for så vidt angår vejledninger til ETSI TS 102 176 ([4]) og til ECRYPT2 D.SPA.x-rapporten ([5]), hvor der findes yderligere anbefalinger vedrørende algoritmer og parametre, der må bruges til elektroniske signaturer.

Anvendelsen af »*transformere*« er begrænset til de nedenfor anførte:

**Kanonikaliseringstransformere**: se tilhørende specifikationerne ovenfor

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

**Filtrering**:

*XPath* (http://www.w3.org/TR/1999/REC-xpath-19991116): af hensyn til kompatibilitet og overensstemmelse med XMLDSig

*XPath Filter 2.0* (http://www.w3.org/2002/06/xmldsig-filter2): som en efterfølger til XPath af hensyn til funktionsdygtigheden

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

**XSLT** (Extensible Stylesheet Language Transformations) **transform**.

ds:KeyInfo element SKAL inkludere underskriverens X.509 v3-digitalcertifikat (dvs. dets værdi og ikke blot en reference til det)

Den signerede signaturegenskab »SigningCertificate« SKAL indeholde digestværdien (CertDigest) og underskriverens IssuerSerial lagret i ds:KeyInfo, og den valgfrie URI i »SigningCertificate«-feltet MÅ IKKE anvendes.

Den signerede signaturegenskab SigningTime er til stede og indeholder UTC udtrykt som xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime)

Elementet DataObjectFormat SKAL VÆRE til stede og indeholde MimeType-subelementet;

Hvis de signaturer, der anvendes af en medlemsstat, er baseret på et kvalificeret certifikat, kan PKI-objekterne (certifikatkæder, tilbagekaldelsesdata, tidsstempler), som indgår i signaturerne, kontrolleres ved hjælp af positivlisten i henhold til Kommissionens beslutning 2009/767/EF for den medlemsstat, der fører tilsyn med eller akkrediterer de certificeringstjenesteudbydere, der har udstedt underskriverens certifikat.

Tabel 1 sammenfatter de specifikationer som en XAdES-BES/EPES-signatur skal opfylde for at være teknisk understøttet af den modtagende medlemsstat.

([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]) Seneste version er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), dateret 30. marts 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

*Tabel 1*

| **XAdES - BES (EPES)** | | **Fælles mindstekrav** |
|---|---|---|
| (ETSI TS 103 903 finder anvendelse med følgende profilerede elementer) | | |
| *M=Mandatory (krav); O=Optional (valgfri); R=Recommended (anbefalet); N=Not used (ikke anvendt)* | | |
| ds: Signature ID | M | |
| ds: SignedInfo | M | |
| ds: CanonicalizationMethod | M | *Alle følgende algoritmer SKAL understøttes ved signaturkontrol, generering BØR begrænses til en af disse:*<br>*- Exclusive XML canonicalization 1.0: http://www.w3.org/TR/xml-exc-c14n/*<br>*- Canonical XML 1.0: http://www.w3.org/TR/2001/REC-XML-c14n-20010315*<br>*- Canonical XML 1.1: http://www.w3.org/2006/12/xml-c14n11*<br>*Andre metoder eller "#WithComments"-versioner af ovenstående metoder BØR IKKE anvendes.* |
| ds: SignatureMethod | M | ***Algorithmer:*** *se gældende nationale love og som vejledning ETSI TS 102 176 samt ECRYPT2 D.SPA.7-rapporten for yderligere anbefalinger.* |
| ds: Reference URI | M | En reference til hvert original dataobjekt signeres (URI'er kan også pege på eksterne objekter), + reference til elementet SignedProperties |
| ds: Transforms | O | *Kontrolapplikationer SKAL understøtte alle følgende transformationer, mens signaturgenereringsapllikationer BØR begrænse anvendelsen af disse transformationer til følgende::*<br>*- Canonicalization transforms: se ovefor*<br>*- Base64 encoding*<br>*- XPath and XPath Filter 2.0*<br>*- Enveloped signature transform*<br>*- XSLT transforms* |
| ds: DigestMethod | M | ***Algoritmer:*** *se gældende national lovgivning samt ETSI TS 102 176 for retningslinjer og ECRYPT2 D.SPA.7-rapporten for yderligere anbefalinger.* |
| ds: DigestValue | M | |
| /ds: Reference | | |
| /ds: SignedInfo | | |
| ds: SignatureValue | M | |
| ds: KeyInfo | M | SKAL indeholde X509-certifikat (SigningCertificate signed property SKAL indeholde digestværdien for dette signer's certificate)<br>Det ANBEFALES at angive certificeringskæde for Signer's certificate som en hjælp til valideringsprocessen (i så fald SKAL der leveres X.509-certifikater). |
| ds: Object | | |
| QualifyingProperties | M | |
| SignedProperties | M | M |
| SignedSignatureProperties | M | M |
| SigningTime | M | UTC (xsd: dateTime). |
| SigningCertificate | M | SKAL indeholde digestværdi for signer's certificate lagret i ds:KeyInfo, og valgfri URI udelades (applikationer KAN søge/finde signer certificate in ds:KeyInfo på grundlag af hash-ækvivalens). |
| SignaturePolicyIdentifier | O | kun for EPES-formularer (og for øvre formularer bygget på basis af EPES-formular) |
| Signature ProductionPlace | O | |
| SignerRole | O | |
| /SignedSignatureProperties | | |
| SignedDataObjectProperties | O | |
| DataObjectFormat | M | Når dette felt bruges, SKAL applikationer sikre, at dataobjekter vises for brugeren i overensstemmelse hermed.<br>Når det bruges, SKAl der anvendes et MimeType child-element. |
| CommitmentTypeIndication | O | |
| AllDataObjectsTimeStamp | O | |
| IndividualDataObjectTimeStamp | O | |
| /SignedDataObjectProperties | | |
| /SignedProperties | | |
| UnsignedProperties | O | |
| UnsignedSignatureProperties | | |
| CounterSignature | O | |
| /UnsignedSignatureProperties | | |
| /UnsignedProperties | | |
| /QualifyingProperties | | |
| /ds: Object | | |
| /ds: Signature | | |
| | | |
| **Signaturtopologi - Pakning af originale filer og signaturer** | | |
| SignatureEnveloped | | Alt SKAL understøttes |
| SignatureEnveloping | | |
| SignatureDetached | | |
| | | |

SEKTION 2 — CAdES-BES/EPES

Signaturen er i overensstemmelse ([1]) med Cryptographic Message Syntax (CMS) signaturspecifikationerne.

Signaturen anvender CAdES-BES (eller -EPES)-signaturattributter som specificeret i ETSI TS 101 733 CadES-specifikationerne ([2]) og er i overensstemmelse med de supplerende specifikationer som angivet i tabel 2 nedenfor.

Alle CadES-attributter, som indgår i beregningen af archive timestamp hash (ETSI TS 101 733 V1.8.1 Annex K), SKAL være i DER-kodning, og alle andre kan være i BER for at forenkle one pass-behandling af CAdES.

MD5 (RFC 1321) MÅ IKKE bruges som en digest-algoritme. Underskrivere henvises til gældende nationale love og for så vidt angår vejledninger til ETSI TS 102 176 ([3]) og til ECRYPT2 D.SPA.x-rapporten ([4]), hvor der findes yderligere anbefalinger vedrørende algoritmer og parametre, der må bruges til elektroniske signaturer.

De signerede attributter SKAL omfatte en reference til underskriverens X.509 v3-digitale certifikat (RFC 5035) og feltet *SignedData.certificates* SKAL indeholde dets værdi.

Den signerede attribut SigningTime SKAL være til stede og SKAL indeholde UTC udtrykt som i http://tools.ietf.org/html/rfc5652#section-11.3.

Den signerede attribut ContentType SKAL være til stede og indeholde id-data (http://tools.ietf.org/html/rfc5652#section-4), hvor datainholdstypen (data content type) er beregnet til at referere til arbitrære oktetstrenge som f.eks. UTF-8 text eller ZIP container med MimeType-subelement.

Hvis de signaturer, der anvendes af en medlemsstat, er baseret på et kvalificeret certifikat, kan PKI-objekterne (certifikatkæder, tilbagekaldelsesdata, tidsstempler), som indgår i signaturerne, kontrolleres ved hjælp af positivlisten i henhold til beslutning 2009/767/EF for den medlemsstat, der fører tilsyn med eller akkrediterer de certificeringstjenesteudbydere, der har udstedt underskriverens 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; Part 1: Hash functions and asymmetric algorithms; Part 2: »Secure channel protocols and algorithms for signature creation devices«.

([4]) Seneste version er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), dateret 30. marts 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

*Tabel 2*

| CAdES - BES (EPES) | | Fælles mindstekrav |
|---|---|---|
| (ETSI TS 101 733 applies with the following profiled elements) | | |
| ASN.1 | | |
| ContentInfo ::= SEQUENCE { | | |
| contentType ContentType, -- id-signedData | | |
| content [0] EXPLICIT ANY DEFINED BY contentType } | | |
| | | |
| *M=Mandatory (krav); O=Optional (valgfri); R=Recommended (anbefalet); N=Not used (ikke anvendt)* | | |
| SignedData ::= SEQUENCE { | | |
| version CMSVersion, | | |
| digestAlgorithms DigestAlgorithmIdentifiers, | M | **Algoritmer**: se gældende nationale love og som vejledning ETSI TS 102 176 samt ECRYPT2 D.SPA.7-rapporten for yderligere anbefalinger. |
| encapContentInfo SEQUENCE { | | |
| eContentType ContentType, | M | id-Data |
| eContent [0] EXPLICIT<br>OCTET STRING OPTIONAL<br>-- not present if signature is detached<br>}, | M/N | Den signerede ContentType-attribut er til stede og indeholder id-data<br>(http://tools.ietf.org/html/rfc5652#section-4), hvor datatype er beregnet til at henvise til arbitrære oktetstrenge som UTF-8 text eller ZIP container med MimeType sub-element |
| -- External Data (if signature detached)* | | hvis adskilt signatur ikke er til stede på anden måde.<br>* Ved eksterne data forstås data, der er beskyttet af en adskilt signatur, der ikke er inkluderet i CAdES signature eContent. Det anbefales at inkludere signerede eksterne data sammen med signaturen i ZIP-fil. |
| certificates [0] IMPLICIT CertificateSet OPTIONAL, | M | SKAL indeholde X509-certifikat fra underskriver. Inkludering af certifikater fra hele certificeringskæden og op til et trust anchor ANBEFALES. |
| crls [1] IMPLICIT RevocationInfoChoices OPTIONAL, | O | |
| signerInfos SET OF | M | Mindst en signerInfo |
| SEQUENCE { -- SignerInfo | | |
| version CMSVersion, | | |
| sid SignerIdentifier, | O | (ikke beskyttet værdi) |
| digestAlgorithm DigestAlgorithmIdentifier, | M | **Algoritmer**: se gældende national lovgivning samt ETSI TS 102 176 for retningslinjer og ECRYPT2 D.SPA.7-rapporten for yderligere anbefalinger. |
| signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF | | |
| SEQUENCE { -- Attribute | M | |
| attrType OBJECT IDENTIFIER, | M/O | SKAL:<br>id-contentType (med id-data)<br>id-messageDigest<br>id-aa-ets-signingCertificateV2 eller id-aa-signingCertificate<br>SKAL: signingTime<br>VALGFRI:<br>id-aa-ets-sigPolicyId<br>Andre valgfrie attributter som defineret i ETSI TS 101 733. |
| attrValues SET OF AttributeValue<br>} OPTIONAL, | | |
| signatureAlgorithm<br>SignatureAlgorithmIdentifier, | | **Algoritmer**: se gældende national lovgivning samt ETSI TS 102 176 for retningslinjer og ECRYPT2 D.SPA.7-rapporten for yderligere anbefalinger. |
| signature OCTET STRING, -- SignatureValue | | |
| unsignedAttrs [1] IMPLICIT SET SIZE<br>(1..MAX) OF | O | |
| SEQUENCE {<br>attrType OBJECT IDENTIFIER,<br>attrValues SET OF<br>AttributeValue<br>} OPTIONAL<br>}<br>} | O | |

SEKTION 3 — PAdES-PART 3 (BES/EPES):

Signaturen SKAL være en PAdES-BES (eller -EPES)-signaturekstension som specificeret i ETSI TS 102 778 PAdES-Part3-specifikationen ([1]) og i overensstemmelse med følgende supplerende specifikationer:

MD5 (RFC 1321) MÅ IKKE anvendes som digest-algoritme. Underskrivere henvises til gældende nationale love og for så vidt angår vejledninger til ETSI TS 102 176 ([2]) og til ECRYPT2 D.SPA.x-rapporten ([3]), hvor der findes yderligere anbefalinger vedrørende algoritmer og parametre, der må bruges til elektroniske signaturer.

De signerede attributter SKAL omfatte en reference til underskriverens X.509 v3-digitale certifikat (RFC 5035) og feltet *SignedData.certificates* SKAL indeholde dets værdi.

([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]) Seneste version er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), dateret 30. marts 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Sigeringstidspunktet angives af værdien af **M** i signaturordbogen.

Hvis de signaturer, der anvendes af en medlemsstat, er baseret på et kvalificeret certifikat, kan PKI-objekterne (certifikatkæder, tilbagekaldelsesdata, tidsstempler), som indgår i signaturerne, kontrolleres ved hjælp af positivlisten i henhold til beslutning 2009/767/EF for den medlemsstat, der fører tilsyn med eller akkrediterer de certificeringstjenesteudbydere, der har udstedt underskriverens certifikat.