**KOMMISJONSBESLUTNING** **2016/EØS/35/49**

**av 25. februar 2011**

**om fastsettelse av minstekrav til behandling over landegrensene av dokumenter som signeres elektronisk av vedkommende myndigheter i henhold til europaparlaments- og rådsdirektiv 2006/123/EF om tjenester i det indre marked**

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

(2011/130/EU)(*)

EUROPAKOMMISJONEN HAR —

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsdirektiv 2006/123/EF av 12. desember 2006 om tjenester i det indre marked([1]), særlig artikkel 8 nr. 3, og

ut fra følgende betraktninger:

1) Tjenesteytere som yter tjenester som faller inn under virkeområdet for direktiv 2006/123/EF, må gjennom de felles kontaktpunktene og på elektronisk måte kunne fullføre de framgangsmåter og formaliteter som er nødvendige for å få tilgang til og utøve sin virksomhet. Innenfor de grenser som er fastsatt i artikkel 5 nr. 3 i direktiv 2006/123/EF, kan det fremdeles være tilfeller der tjenesteytere må sende originaldokumenter, bekreftede kopier eller bekreftede oversettelser når slike framgangsmåter og formaliteter fullføres. I disse tilfellene kan tjenesteytere ha behov for å oversende dokumenter som er elektronisk signert av vedkommende myndigheter.

2) Bruken over landegrensene av avanserte elektroniske signaturer som er basert på et kvalifisert sertifikat, er blitt forenklet ved kommisjonsvedtak 2009/767/EF av 16. oktober 2009 om fastsettelse av tiltak for å forenkle bruken av elektroniske framgangsmåter ved hjelp av «felles kontaktpunkter» i samsvar med europaparlaments- og rådsdirektiv 2006/123/EF om tjenester i det indre marked([2]), som bl.a. forplikter medlemsstatene til å utføre risikovurderinger før de krever disse elektroniske signaturene fra tjenesteytere og fastsetter regler for medlemsstatenes anerkjennelse av avanserte elektroniske signaturer basert på kvalifiserte sertifikater, opprettet med eller uten et sikkert signaturframstillingssystem. I vedtak 2009/767/EF omhandles imidlertid ikke formater for elektroniske signaturer i dokumenter som er utstedt av vedkommende myndigheter, og som tjenesteytere må oversende når de fullfører de relevante framgangsmåter og formaliteter.

3) Ettersom vedkommende myndigheter i medlemsstatene for øyeblikket benytter forskjellige formater for avanserte elektroniske signaturer til å signere sine dokumenter elektronisk, kan mottakerstaten som skal behandle disse dokumentene, støte på tekniske problemer som følge av at signaturformatene varierer. For å gjøre det mulig for tjenesteytere å fullføre sine framgangsmåter og formaliteter elektronisk over landegrensene, må det sikres at minst et visst antall formater for avanserte elektroniske signaturer kan støttes teknisk av medlemsstatene når disse mottar dokumenter som er signert elektronisk av vedkommende myndigheter i andre medlemsstater. Ved å definere et antall formater for avanserte elektroniske signaturer som kan støttes teknisk av mottakerstaten, vil det gis mulighet for større grad av automatisering og forbedret samvirkingsevne mellom elektroniske framgangsmåter.

4) Medlemsstater der vedkommende myndigheter benytter andre formater for elektroniske signaturer enn dem som vanligvis støttes, kan ha innført valideringsmetoder som gjør det mulig å verifisere deres signaturer også over landegrensene. I slike tilfeller, og for at mottakerstater skal kunne stole på disse valideringsverktøyene, må opplysninger om disse verktøyene gjøres tilgjengelige på en enkel måte, med mindre de nødvendige opplysningene inngår direkte i de elektroniske signaturene eller i de elektroniske konvoluttene.

5) Denne beslutning berører ikke medlemsstatenes definisjon av hva som utgjør en original, en bekreftet kopi eller en bekreftet oversettelse. Beslutningens formål er begrenset til å forenkle verifiseringen av elektroniske signaturer dersom disse benyttes i originaler, bekreftede kopier eller bekreftede oversettelser som det kan være nødvendig for tjenesteyterne å oversende via de felles kontaktpunktene.

(*) Denne fellesskapsrettsakten, kunngjort i EUT L 53 av 26.2.2011, s. 66, er omhandlet i EØS-komiteens beslutning nr. 21/2012 av 10. februar 2012 om endring av EØS-avtalens vedlegg X (Generelle tjenester), se EØS-tillegget til *Den europeiske unions tidende* nr. 34 av 21.6.2012, s. 32.

([1]) EUT L 376 av 27.12.2006, s. 36.

([2]) EUT L 274 av 20.10.2009, s. 36.

6) For at medlemsstatene skal kunne innføre de nødvendige tekniske verktøyene, bør denne beslutning få anvendelse fra 1. august 2011.

7) Tiltakene fastsatt i denne beslutning er i samsvar med uttalelse fra Tjenestedirektivkomiteen —

TRUFFET DENNE BESLUTNING:

*Artikkel 1*

**Referanseformat for elektroniske signaturer**

1. Medlemsstatene skal skaffe til veie de nødvendige tekniske midler som gjør det mulig for dem å behandle elektronisk signerte dokumenter som tjenesteytere oversender i forbindelse med fullføring av framgangsmåter og formaliteter gjennom felles kontaktpunkter i henhold til artikkel 8 i direktiv 2006/123/EF, og som er signert av vedkommende myndigheter i andre medlemsstater med en avansert elektronisk XML-, CMS- eller PDF-signatur i BES- eller EPES-format som oppfyller de tekniske spesifikasjonene angitt i vedlegget.

2. Medlemsstater der vedkommende myndigheter signerer dokumentene nevnt i nr. 1 ved hjelp av elektroniske signaturer i et annet format enn dem som nevnes i samme nummer, skal underrette Kommisjonen om de valideringsmulighetene som foreligger, slik at andre medlemsstater kan validere mottatte elektroniske signaturer direktekoplet, gratis og på en måte som er forståelig for personer som har et annet morsmål, med mindre de opplysningene som kreves, allerede inngår i dokumentet, i den elektroniske signaturen eller i den elektroniske konvolutten. Kommisjonen skal gjøre disse opplysningene tilgjengelige for alle medlemsstatene.

*Artikkel 2*

**Anvendelse**

Denne beslutning får anvendelse fra 1. august 2011.

*Artikkel 3*

**Mottakere**

Denne beslutning er rettet til medlemsstatene.

Utferdiget i Brussel, 25. februar 2011.

*For Kommisjonen*

Michel BARNIER

*Medlem av Kommisjonen*

*VEDLEGG*

**Spesifikasjoner for en avansert elektronisk XML-, CMS- eller PDF-signatur som skal støttes teknisk av mottakerstaten**

I den følgende delen av dokumentet skal nøkkelordene «MÅ», «MÅ IKKE», «PÅKREVD», «SKAL», «SKAL IKKE», «BØR», «BØR IKKE», «ANBEFALT», «KAN» og «VALGFRI» tolkes som beskrevet i RFC 2119([1]).

DEL 1 — XAdES-BES/EPES

Signaturen er i samsvar med W3Cs spesifikasjoner for XML-signaturer([2]).

Signaturen MÅ minst ha et signaturformat av typen XAdES-BES (eller -EPES), som angitt i XAdES-spesifikasjonene for ETSI TS 101 903([3]), og dessuten oppfylle alle følgende tilleggsspesifikasjoner:

Metoden ds:CanonicalizationMethod, som angir hvilken kanonikaliseringsalgoritme som anvendes på SignedInfo-elementet før signaturberegningene utføres, identifiserer bare én av følgende algoritmer:

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

Andre algoritmer eller versjoner av ovennevnte algoritmer «med kommentarer» BØR IKKE benyttes til framstilling av signaturer, men BØR støttes for fortsatt samvirkingsevne ved verifisering av signaturen.

MD5 (RFC 1321) MÅ IKKE benyttes som sjekksumalgoritme. Underskrivere henvises til gjeldende nasjonal lovgivning og, når det gjelder retningslinjer, til ETSI TS 102 176([4]) og rapporten ECRYPT2 D.SPA.x([5]) for videre anbefalinger om algoritmer og parametrer som kan benyttes til elektroniske signaturer.

Bruken av *transformasjoner* begrenses til dem som er oppført nedenfor:

**Kanonikaliseringstransformasjoner**: Se tilhørende spesifikasjoner ovenfor.

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

**Filtrering**:

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

*XPath Filter 2.0* (http://www.w3.org/2002/06/xmldsig-filter2): som en etterfølger til XPath av hensyn til funksjonsdyktighet.

**Innpakket signatur-transformasjon***:* (http://www.w3.org/2000/09/xmldsig#enveloped-signature).

**XSLT-transformasjon** (stilmal).

Elementet ds:KeyInfo MÅ omfatte underskriverens digitale X.509 v3-sertifikat (dvs. dets verdi, og ikke bare en henvisning til det).

Signaturegenskapen som signeres med «SigningCertificate», MÅ inneholde sjekksumverdien (CertDigest) og IssuerSerial for underskriverens sertifikat lagret i ds:KeyInfo, og den valgfrie URI i feltet «SigningCertificate» MÅ IKKE benyttes.

Signaturegenskapen som signeres med SigningTime, foreligger, og inneholder UTC uttrykt som xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

Elementet DataObjectFormat MÅ foreligge og inneholde et MimeType-underelement.

Dersom de signaturene som benyttes av medlemsstatene, er basert på et kvalifisert sertifikat, kan PKI-objektene (sertifikatkjeder, tilbakekallingsdata, tidsstempler) som inngår i signaturene, verifiseres ved hjelp av pålitelighetslisten, i samsvar med kommisjonsvedtak 2009/767/EF, til den medlemsstaten som fører tilsyn med eller akkrediterer den CSP-en som har utstedt underskriverens sertifikat.

I tabell 1 oppsummeres de spesifikasjonene som en XAdES-BES/EPES-signatur må oppfylle for at den skal kunne støttes teknisk av mottakerstaten.

([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]) Siste versjon er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010) av 30. mars 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

*Tabell 1*

| **XAdES – BES (EPES)** | | **Felles minstekrav** |
|---|---|---|
| (ETSI TS 103 903 gjelder med følgende profilelementer) | | |
| *O=Obligatorisk, V=Valgfritt, A=Anbefalt, B=Brukes ikke* | | |
| ds: Signature ID | O | |
| ds: SignedInfo | O | |
| ds: CanonicalizationMethod | O | *Alle algoritmene nedenfor MÅ støttes ved verifisering av signaturen, framstillingen BØR avgrenses til én av disse:*<br>*- Exclusive XML canonicalization 1.0: http://www.w3org/TR/xml-exc-c14n/*<br>*- Canonical XML 1.0: http://www.w3org/TR/2001/REC-XML-c14n-20010315*<br>*- Canonical XML 1.1: http:/www.w3org/2006/12/xml-c14n11*<br>*Andre metoder eller «#WithComments»-versjoner av metodene ovenfor BØR IKKE benyttes.* |
| ds: SignatureMethod | O | ***Algoritmer**: Se gjeldende nasjonal lovgivning, og for retningslinjer, se ETSI TS 102 176 og rapporten ECRYPT2 D.SPA.7 for videre anbefalinger.* |
| ds: Reference URI | O | Én henvisning til hvert originale dataobjekt som skal signeres (URI-er kan også peke til eksterne objekter), + henvisning til SignedProperties-element |
| ds: Transforms | V | *Verifiseringsapplikasjoner MÅ støtte alle de følgende transformasjoner, mens applikasjoner for signaturframstilling BØR begrense bruken av disse transformasjonene til følgende:*<br>*- Kanonikaliseringstransformasjoner: se ovenfor*<br>*- Base64-koding*<br>*- XPath og XPath Filter 2.0*<br>*- Innpakket signatur-transformasjon*<br>*- XSLT-transformasjoner* |
| ds: DigestMethod | O | ***Algoritmer**: Se gjeldende nasjonal lovgivning, og for retningslinjer, se ETSI TS 102 176 og rapporten ECRYPT2 D.SPA.7 for videre anbefalinger.* |
| ds: DigestValue | O | |
| /ds: Reference | | |
| /ds: SignedInfo | | |
| ds: SignatureValue | O | |
| ds: KeyInfo | O | Må inneholde X509-sertifikat (signaturegenskapen SigningCertificate MÅ inneholde sjekksumverdien for denne underskriverens sertifikat)<br>Det ANBEFALES at sertifiseringskjeden for underskriverens sertifikat angis, som en hjelp til å forenkle valideringsprosessen (i så fall MÅ X.509-sertifikater leveres). |
| ds: Object | | |
| QualifyingProperties | O | |
| SingedProperties | O | O |
| SignedSignatureProperties | O | O |
| SigningTime | O | UTC (xsd: dateTime) |
| SigningCertificate | O | MÅ inneholde sjekksumverdien for underskriverens sertifikat, som er lagret i ds: KeyInfo, og valgfri URI utelates (applikasjoner KAN lete etter / finne underskriverens sertifikat i ds: KeyInfo på grunnlag av hash-ekvivalens). |
| SignaturePolicyIdentifier | V | Bare for EPES-format (og for høyere formater basert på EPES-formatet). |
| Signature ProductionPlace | V | |
| SignerRole | V | |
| /SignedSignatureProperties | | |
| SignedDataObjectProperties | V | |
| DataObjectFormat | O | Når dette feltet benyttes, SKAL applikasjoner sikre at dataobjekter vises for brukeren på samme måte.<br>Når det benyttes, MÅ et underordnet MimeType-element benyttes. |
| CommitmentTypeIndication | V | |
| AllDataObjectsTimeStamp | V | |
| IndividualDataObjectTime/ Stamp | V | |
| /SignedDataObjectProperties | | |
| /SignedProperties | | |
| UnsignedProperties | V | |
| UnsignedSignatureProperties | | |
| CounterSignature | V | |
| /UnsignedSignatureProperties | | |
| /UnsignedProperties | | |
| /QualifyingProperties | | |
| /ds: Object | | |
| /ds: Signature | | |
| | | |
| **Signaturtopologi – pakking av signerte originalfiler og av signaturer** | | |
| SignatureEnveloped | | Alle MÅ støttes |
| SignatureEnveloping | | |
| SignatureDetached | | |
| | | |

DEL 2 — CAdES-BES/EPES

Signaturen er i samsvar med spesifikasjonene for Cryptographic Message Syntax-signatur (CMS-signatur)([1]).

Signaturen benytter signaturattributter for CAdES-BES (eller -EPES) som angitt i spesifikasjonene for ETSI TS 101 733 CAdES([2]), og er i samsvar med tilleggsspesifikasjonene angitt i tabell 2 nedenfor.

Alle CAdES-attributter som inngår i hash-beregningen av arkivets tidsstempel (ETSI TS 101 733 V1.8.1 Annex K), MÅ være DER-kodet, og alle andre kan være BER-kodet, for å forenkle ettrinnsbehandlingen av CAdES.

MD5 (RFC 1321) MÅ IKKE benyttes som sjekksumalgoritme. Underskrivere henvises til gjeldende nasjonal lovgivning og, når det gjelder retningslinjer, til ETSI TS 102 176([3]) og rapporten ECRYPT2 D.SPA.x([4]) for videre anbefalinger om algoritmer og parametrer som kan benyttes til elektroniske signaturer.

Signeringsattributtene MÅ inneholde en henvisning til underskriverens digitale X.509 v3-sertifikat (RFC 5035), og feltet *SignedData.certificates* MÅ inneholde dettes verdi.

Signeringsattributtene SigningTime MÅ foreligge og MÅ inneholde UTC uttrykt som i http://tools.ietf.org/html/rfc5652#section-11.3.

Signeringsattributtet ContentType MÅ foreligge og inneholde id-data (http://tools.ietf.org/html/rfc5652#section-4) der typen datainnhold er beregnet på å henvise til arbitrære oktettstrenger, f.eks. UTF-8-tekst eller en ZIP-container med et MimeType-underelement.

Dersom de signaturene som benyttes av medlemsstatene, er basert på et kvalifisert sertifikat, kan PKI-objektene (sertifikatkjeder, tilbakekallingsdata, tidsstempler) som inngår i signaturene, verifiseres ved hjelp av pålitelighetslisten, i samsvar med kommisjonsvedtak 2009/767/EF, til den medlemsstaten som fører tilsyn med eller akkrediterer den CSP-en som har utstedt underskriverens sertifikat.

([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 v1.4.1: XML Advanced Electronic Signatures (XAdES).

([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]) Siste versjon er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010) av 30. mars 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

*Tabell 2*

| | | |
|---|---|---|
| **CAdES** | | **Felles minstekrav** |
| (ETSI TS 101 733 gjelder med følgende profilelementer) | | |
| **ASN.1** | | |
| ContentInfo :: = SEQUENCE { | | |
| contentType ContentType, -- id-signedData | | |
| Content [0] EXPLICIT ANY DEFINED BY content Type } | | |
| | | |
| *O=Obligatorisk, V=Valgfritt, A=Anbefalt, B=Brukes ikke* | | |
| SignedData :: = SEQUENCE { | | |
| Version CMSVersion, | | |
| digestAlgorithms DigestAlgorithmIdentifiers, | O | **Algoritmer:** Se gjeldende nasjonal lovgivning, og for retningslinjer, se ETSI TS 102 176 og rapporten ECRYPT2 D.SPA.7 for videre anbefalinger. |
| encapContentInfo SEQUENCE { | | |
| eContentType ContentType, | O | Id-Data |
| eContent [0] EXPLICIT OCTET STRING OPTIONAL -- foreligger ikke dersom signaturen er atskilt }, | O/B | Signeringsattributtet ContentType foreligger og inneholder id-data. (http://tools.ietf.org/html/rfc5652#section-4) der typen datainnhold er beregnet på å henvise til arbitrære oktettstrenger, f.eks. UTF-8-tekst eller en ZIP-container med et MimeType-underelement. |
| -- External Data (dersom signaturen er atskilt)* | | Dersom en atskilt signatur ikke foreligger på annen måte.<br>* Eksterne data betyr data som er beskyttet av en atskilt signatur som ikke inngår i e-innholdet til CAdES-signaturen. Det anbefales at signerte data inkluderes sammen med signaturen i en ZIP-fil. |
| Certificates [0] IMPLICIT CertificateSet OPTIONAL, | O | **MÅ** inneholde X509-sertifikat fra underskriveren. Det ANBEFALES at sertifikater fra hele sertifiseringskjeden til og med et tillitsanker inkluderes. |
| crls [1] IMPLICIT RevocationInfoChoices OPTIONAL, | V | |
| signerInfos SET OF | O | Minst én signerInfo |
| SEQUENCE { -- SignerInfo | | |
| version CMSVersion, | | |
| sid SignerIdentifier, | V | (Ikke beskyttet verdi) |
| digestAlgorithm DigestAlgorithmIdentifier | O | **Algoritmer:** se gjeldende nasjonal lovgivning, og for retningslinjer, se ETSI TS 102 176 og rapporten ECRYPT2 D.SPA.7 for videre anbefalinger. |
| signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF | | |
| SEQUENCE { -- Attribute | O | |
| attrType OBJECT IDENTIFIER, | O/V | **MÅ:**<br>Id-contentType (med data)<br>Id-messagerDigest<br>Id-aa-ets-signingCertificate V2 eller id-aa-signingCertificate<br>MÅ: signingTime<br>**VALGFRITT:**<br>Id-aa-ets-sigPolicyId<br>Andre valgfrie attributter som definert i ETSI TS 101 733. |
| attrValues SET OF AttributeValue }, OPTIONAL | | |
| signatureAlgorithm SignatureAlgorithmIdentifier, | | **Algoritmer:** Se gjeldende nasjonal lovgivning, og for retningslinjer, se ETSI TS 102 176 og rapporten ECRYPT2 D.SPA.7 for videre anbefalinger. |
| Signature OCTET STRING, -- SignatureValue | | |
| unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF | V | |
| SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } } } | V | |
| | | |

DEL 3 — PAdES-PART 3 (BES/EPES)

Signaturen MÅ ha en signaturutvidelse av typen PAdES-BES (eller -EPES), som angitt i PAdES-Part3-spesifikasjonene for ETSI TS 102 778([1]), og dessuten oppfylle alle følgende tilleggsspesifikasjoner:

MD5 (RFC 1321) MÅ IKKE benyttes som sjekksumalgoritme. Underskrivere henvises til gjeldende nasjonal lovgivning og, når det gjelder retningslinjer, til ETSI TS 102 176([2]) og rapporten ECRYPT2 D.SPA.x([3]) for videre anbefalinger om algoritmer og parametrer som kan benyttes til elektroniske signaturer.

Signeringsattributtene MÅ inneholde en henvisning til underskriverens digitale X.509 v3-sertifikat (RFC 5035), og feltet *SignedData.certificates* MÅ inneholde dettes verdi.

([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]) Siste versjon er D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010) av 30. mars 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Signeringstidspunktet angis ved verdien til oppføringen *M* i signaturkatalogen.

Dersom de signaturene som benyttes av medlemsstatene, er basert på et kvalifisert sertifikat, kan PKI-objektene (sertifikatkjeder, tilbakekallingsdata, tidsstempler) som inngår i signaturene, verifiseres ved hjelp av pålitelighetslisten, i samsvar med vedtak 2009/767/EF, til den medlemsstaten som fører tilsyn med eller akkrediterer den CSP-en som har utstedt underskriverens sertifikat.