PÄÄTÖKSET

KOMISSION PÄÄTÖS,

annettu 25 päivänä helmikuuta 2011,

palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY nojalla toimivaltaisten viranomaisten sähköisesti allekirjoittamien asiakirjojen maiden rajat ylittävää käsittelyä koskevista vähimmäisvaatimuksista

(tiedoksiannettu numerolla K(2011) 1081)

(ETA:n kannalta merkityksellinen teksti)

(2011/130/EU)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon palveluista sisämarkkinoilla 12 päivänä joulukuuta 2006 annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY ([1]) ja erityisesti sen 8 artiklan 3 kohdan,

sekä katsoo seuraavaa:

(1) Palveluntarjoajien, joiden palvelut kuuluvat direktiivin 2006/123/EY soveltamisalaan, on voitava hoitaa toimintansa aloittamisen ja harjoittamisen edellyttämät menettelyt ja muodollisuudet keskitetyn asiointipisteen kautta sähköisesti. Direktiivin 2006/123/EY 5 artiklan 3 kohdassa säädetyissä rajoissa voi edelleen ilmetä tapauksia, joissa palveluntarjoajien on toimitettava tällaisten menettelyjen ja muodollisuuksien yhteydessä alkuperäisiä asiakirjoja, oikeaksi todistettuja jäljennöksiä tai virallisia käännöksiä. Näissä tapauksissa palveluntarjoajat saattavat joutua toimittamaan asiakirjoja toimivaltaisten viranomaisten sähköisellä allekirjoituksella varustettuina.

(2) Hyväksyttyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten käyttöä maiden rajojen yli helpotetaan toimenpiteistä sähköisten menettelyjen käytön edistämiseksi keskitettyjä asiointipisteitä käyttäen palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY mukaisesti 16 päivänä lokakuuta 2009 tehdyllä komission päätöksellä 2009/767/EY ([2]), jossa muun muassa velvoitetaan jäsenvaltiot suorittamaan riskinarviointeja ennen kuin ne edellyttävät palveluntarjoajilta tällaisia sähköisiä allekirjoituksia sekä asetetaan säännöt, joiden mukaisesti jäsenvaltiot hyväksyvät turvallisilla allekirjoitusten luomismenetelmillä tai muulla tavoin luotuja hyväksyttyyn varmenteeseen perustuvia kehittyneitä sähköisiä allekirjoituksia. Päätöksessä 2009/767/EY ei kuitenkaan käsitellä sähköisten allekirjoitusten muotoa toimivaltaisten viranomaisten myöntämissä asiakirjoissa, joita palveluntarjoajien on toimitettava hoitaessaan tarvittavia menettelyjä ja muodollisuuksia.

(3) Koska jäsenvaltioiden toimivaltaiset viranomaiset käyttävät tällä hetkellä asiakirjojaan sähköisesti allekirjoittaessaan erimuotoisia kehittyneitä sähköisiä allekirjoituksia, kyseisiä asiakirjoja käsittelemään joutuvat vastaanottavat jäsenvaltiot saattavat kohdata allekirjoitusmuotojen eroista johtuvia teknisiä ongelmia. Jotta palveluntarjoajat voisivat hoitaa menettelynsä ja muodollisuutensa rajojen yli sähköisesti, on varmistettava, että jäsenvaltioilla on tekniset valmiudet käsitellä ainakin joitain kehittyneiden sähköisten allekirjoitusten muotoja vastaanottaessaan muiden jäsenvaltioiden toimivaltaisten viranomaisten sähköisesti allekirjoittamia asiakirjoja. Määrittelemällä joukko kehittyneiden sähköisten allekirjoitusten muotoja, joiden käsittelyyn vastaanottavalla jäsenvaltiolla on oltava valmiudet, mahdollistettaisiin pidemmälle menevä automaatio ja parannettaisiin sähköisten menettelyjen yhteentoimivuutta rajojen yli.

(4) Jäsenvaltiot, joiden toimivaltaiset viranomaiset käyttävät muita kuin yleisesti tuettuja sähköisten allekirjoitusten muotoja, ovat saattaneet ottaa käyttöön validointimenetelmiä, jotka mahdollistavat niiden allekirjoitusten todentamisen myös rajojen yli. Näissä tapauksissa, ja jotta vastaanottavat jäsenvaltiot voisivat hyödyntää kyseisiä validointimenetelmiä, on tarpeen asettaa menetelmiä koskevat tiedot helposti saataville, elleivät tarvittavat tiedot sisälly jo suoraan sähköisiin asiakirjoihin, sähköisiin allekirjoituksiin tai sähköisen asiakirjan siirtosovellukseen.

(5) Tämä päätös ei vaikuta siihen, miten jäsenvaltiot määrittelevät alkuperäiskappaleen, oikeaksi todistetun jäljennöksen tai virallisen käännöksen. Päätöksen tavoitteena on yksinomaan helpottaa sähköisten allekirjoitusten todentamista, kun niitä käytetään alkuperäiskappaleissa, oikeaksi todistetuissa jäljennöksissä tai virallisissa käännöksissä, joita palveluntarjoajat saattavat joutua toimittamaan keskitettyjen asiointipisteiden kautta.

([1]) EUVL L 376, 27.12.2006, s. 36.
([2]) EUVL L 274, 20.10.2009, s. 36.

(6) Jotta jäsenvaltioille jää riittävästi aikaa toteuttaa tarvittavat tekniset ratkaisut, tätä päätöstä on asianmukaista soveltaa 1 päivästä elokuuta 2011.

(7) Tässä päätöksessä säädetyt toimenpiteet ovat palveludirektiivikomitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Viitemuoto sähköisille allekirjoituksille

1. Jäsenvaltioiden on toteutettava tarvittavat tekniset valmiudet käsitellä sähköisesti allekirjoitettuja asiakirjoja, joita palveluntarjoajat toimittavat keskitetyn asiointipisteen kautta hoitaessaan menettelyjä ja muodollisuuksia direktiivin 2006/123/EY 8 artiklassa tarkoitetulla tavalla, ja jotka toisen jäsenvaltion toimivaltaiset viranomaiset ovat allekirjoittaneet BES- tai EPES-muotoisella kehittyneellä sähköisellä XML-, CMS- tai PDF-allekirjoituksella, joka vastaa liitteessä esitettyjä teknisiä eritelmiä.

2. Jäsenvaltioiden, joiden toimivaltaiset viranomaiset allekirjoittavat 1 kohdassa tarkoitettuja asiakirjoja muunlaisella kuin kyseisessä kohdassa tarkoitetulla sähköisellä allekirjoituksella, on ilmoitettava komissiolle olemassa olevista validointimahdollisuuksista, joiden avulla muut jäsenvaltiot voivat validoida vastaanotetut sähköiset allekirjoitukset verkossa veloituksetta ja muunkielisten käyttäjien ymmärrettävissä olevalla tavalla, ellei tarvittavia tietoja jo esitetä itse asiakirjassa, sähköisessä allekirjoituksessa tai sähköisen asiakirjan siirtosovelluksessa. Komissio välittää kyseiset tiedot kaikille jäsenvaltioille.

2 artikla

Soveltaminen

Tätä päätöstä sovelletaan 1 päivästä elokuuta 2011.

3 artikla

Osoitus

Tämä päätös on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä 25 päivänä helmikuuta 2011.

Komission puolesta

Michel BARNIER

Komission jäsen

LIITE

Eritelmät kehittyneille sähköisille XML-, CMS- tai PDF-allekirjoituksille, joiden käsittelyyn vastaanottavalla jäsenvaltiolla on oltava tekniset valmiudet

Asiakirjan seuraavassa osassa käytetyt avainsanat PITÄÄ (MUST, SHALL), EI SAA (MUST NOT, SHALL NOT) ja PAKOLLINEN (REQUIRED), PITÄISI (SHOULD), EI PITÄISI (SHOULD NOT), SUOSITELTAVA (RECOMMENDED), SAA (MAY) ja VAPAAEHTOINEN (OPTIONAL) tulkitaan asiakirjassa RFC 2119 ([1]) kuvatulla tavalla.

OSIO 1 – XAdES-BES/EPES:

Allekirjoitus on W3C:n XML Signature -eritelmien ([2]) mukainen.

Allekirjoituksen PITÄÄ olla muodoltaan vähintään XAdES-BES (tai XAdES-EPES), siten kuin ne on määritelty XAdES-eritelmissä asiakirjassa ETSI TS 101 903 ([3]), ja se vastaa kaikkia seuraavia lisäeritelmiä:

Elementissä ds:CanonicalizationMethod, joka ilmaisee ennen allekirjoituksen laskemista SignedInfo-elementtiin sovellettavan kanonikalisointialgoritmin, ilmaistaan ainoastaan jokin seuraavista algoritmeistä:

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

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

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

Muita algoritmejä tai edellä lueteltujen algoritmien kommentteja poistamattomia versioita EI PITÄISI käyttää allekirjoituksen luomisessa, mutta niitä PITÄISI tukea allekirjoituksen todentamisessa jäännösyhteentoimivuuden mahdollistamiseksi.

Tiivisteen laskemiseen EI SAA käyttää MD5-algoritmia (RFC 1321). Allekirjoittajia kehotetaan tutustumaan sovellettaviin kansallisiin lakeihin ja ohjeistojen osalta asiakirjaan ETSI TS 102 176 ([4]) sekä ECRYPT2 D.SPA.x -raporttiin ([5]), joka sisältää lisää suosituksia sähköisissä allekirjoituksissa hyväksyttävistä algoritmeista ja parametreista.

Muunnosten (*transforms*) käyttö on rajattu seuraaviin:

Kanonikalisointimuunnokset: ks. asiaa koskevat eritelmät edellä;

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

Kohdistus:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): yhteensopivuussyistä ja XMLDSig-formaatin mukaisuuden mahdollistamiseksi;

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): Xpath-menetelmän seuraajana suorituskykysyistä;

Kapseloitu allekirjoitus -muunnos: (http://www.w3.org/2000/09/xmldsig#enveloped-signature);

XSLT-muunnos (tyylisäännöstö).

ds:KeyInfo-elementin PITÄÄ sisältää allekirjoittajan digitaalinen X.509 v3 -varmenne (eli sen arvo, ei pelkästään viittausta siihen).

Allekirjoitetun "SigningCertificate"-allekirjoitusominaisuuden PITÄÄ sisältää allekirjoittajan ds:KeyInfo-elementtiin tallennetun varmenteen tiivistearvo (CertDigest) ja IssuerSerial-tunniste, ja "SigningCertificate"-kentässä EI SAA käyttää vapaaehtoista URI-osoitetta.

Allekirjoitettu SigningTime-allekirjoitusominaisuus on käytössä ja sisältää UTC-ajan ilmaistuna muodossa xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

DataObjectFormat-elementin PITÄÄ olla käytössä ja sisältää MimeType-alielementti.

Jos jäsenvaltion käyttämät allekirjoitukset perustuvat hyväksyttyyn varmenteeseen, allekirjoituksiin sisältyvät PKI-objektit (varmenneketjut, sulkutiedot, aikaleimat) ovat todennettavissa päätöksen 2009/767/EY mukaisesti käyttäen sen maan "luotettavaa luetteloa", joka vastaa allekirjoittajan varmenteen myöntäneen varmennepalvelujen tarjoajan valvonnasta tai akkreditoinnista.

Taulukossa 1 esitetään tiivistetysti eritelmät, joiden mukainen XAdES-BES/EPES-allekirjoituksen on oltava, jotta vastaanottavalla jäsenvaltiolla on tekniset valmiudet käsitellä sitä.

([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]) Viimeisin versio on D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), päivätty 30.3.2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Taulukko 1

XAdES - BES (EPES)		**Yhteiset vähimmäisvaatimukset**
(ETSI TS 103 903, seuraavilla kuvatuilla elementeillä)		
P=Pakollinen; V=Vapaaehtoinen; S=Suositeltu; E=Ei käytössä		
ds: Signature ID	P	
ds: SignedInfo	P	
ds: CanonicalizationMethod	P	*Allekirjoituksen todentamisessa PITÄÄ tukea kaikkia seuraavia algoritmeja, mutta luomisessa PITÄISI pidättäytyä vain yhdessä niistä:* *- 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* *Muita menetelmiä tai edellä mainittujen "#WithComments"-versioita EI PITÄISI käyttää.*
ds: SignatureMethod	P	***Algoritmit:*** *sovellettavan kansallisen lainsäädännön mukaisesti; ohjeistusta ETSI TS 102 176 -asiakirjassa ja lisäsuosituksia ECRYPT2 D.SPA.7 -raportissa.*
ds: Reference URI	P	Yksi viittaus jokaiseen alkuperäiseen allekirjoitettavaan dataobjektiin (URI-osoitteilla voidaan viitata myös ulkoisiin objekteihin) + viittaus SignedProperties-elementtiin
ds: Transforms	V	*Todentavien sovellusten PITÄÄ tukea kaikkia seuraavia muunnoksia, kun taas allekirjoituksen luontisovelluksen PITÄISI sallia vain yksi niistä:* *- Kanonikalisointimuunnokset: ks. edellä* *- Base64-koodaus* *- XPath ja XPath Filter 2.0* *- Kapseloitu allekirjoitus -muunnos* *- XSLT-muunnokset*
ds: DigestMethod	P	***Algoritmit:*** *sovellettavan kansallisen lainsäädännön mukaisesti; ohjeistusta ETSI TS 102 176 -asiakirjassa ja lisäsuosituksia ECRYPT2 D.SPA.7 -raportissa .*
ds: DigestValue	P	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	P	
ds: KeyInfo	P	Tämän PITÄÄ sisältää X509-varmenne (allekirjoitetun SigningCertificate-ominaisuuden PITÄÄ sisältää kyseisen allekirjoittajan varmenteen tiivistearvo). Validointiprosessin helpottamiseksi on SUOSITELTAVAA ilmoittaa allekirjoittajan varmenteen varmentamisketju (tällöin PITÄÄ antaa X.509-varmenteet).
ds: Object		
QualifyingProperties	P	
SignedProperties	P	P
SignedSignatureProperties	P	P
SigningTime	P	UTC (xsd: dateTime).
SigningCertificate	P	Tämän PITÄÄ sisältää allekirjoittajan varmenteen tiivistearvo tallennettuna ds:KeyInfo-elementtiin, ja vapaaehtoinen URI jätetään pois (sovellus SAA hakea allekirjoittajan varmennetta ds:KeyInfo-elementistä hash-arvon vastaavuuden perusteella).
SignaturePolicyIdentifier	V	Vain EPES-tyypissä (ja EPES-tyypille rakentuvissa ylemmän tason tyypeissä)
Signature ProductionPlace	V	
SignerRole	V	
/SignedSignatureProperties		
SignedDataObjectProperties	V	
DataObjectFormat	P	Jos tätä kenttää käytetään, sovelluksen PITÄÄ varmistaa, että dataobjektit näkyvät käyttäjälle asianmukaisesti. Jos käytetään, PITÄÄ käyttää myös MimeType-alielementtiä.
CommitmentTypeIndication	V	
AllDataObjectsTimeStamp	V	
IndividualDataObjectTimeStamp	V	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	V	
UnsignedSignatureProperties		
CounterSignature	V	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Allekirjoituksen topologia - Allekirjoitettujen alkuperäistiedostojen ja allekirjoitusten paketointi		
SignatureEnveloped		Kaikkia näitä PITÄÄ tukea
SignatureEnveloping		
SignatureDetached		

OSIO 2 – CAdES-BES/EPES:

Allekirjoitus on Cryptographic Message Syntax (CMS) -eritelmien ([1]) mukainen.

Allekirjoitus käyttää CAdES-BES (tai CAdES-EPES) allekirjoitusattribuutteja ETSI TS 101 733 CAdES -eritelmissä ([2]) määritellyllä tavalla ja vastaa jäljempänä taulukossa 2 esitettyjä lisäeritelmiä.

Kaikkien arkistoaikaleiman hash-laskennassa (ETSI TS 101 733 V1.8.1 Annex K) käytettävien CadES-attribuuttien PITÄÄ olla DER-koodattuja ja muut voivat olla BER-koodattuja CAdESin kertaläpäisyprosessin yksinkertaistamiseksi.

Tiivisteen laskemiseen EI SAA käyttää MD5-algoritmia (RFC 1321). Allekirjoittajia kehotetaan tutustumaan sovellettaviin kansallisiin lakeihin ja ohjeistojen osalta asiakirjaan ETSI TS 102 176 ([3]) sekä ECRYPT2 D.SPA.x -raporttiin ([4]), joka sisältää lisää suosituksia sähköisissä allekirjoituksissa hyväksyttävistä algoritmeista ja parametreista.

Allekirjoitettujen attribuuttien PITÄÄ sisältää viittaus allekirjoittajan digitaaliseen X.509 v3 -varmenteeseen (RFC 5035) ja *SignedData.certificates*-kentän PITÄÄ sisältää sen arvo.

Allekirjoitettu SigningTime-attribuutti PITÄÄ ilmoittaa ja sen PITÄÄ sisältää UTC-aika ilmaistuna asiakirjassa http://tools.ietf.org/html/rfc5652#section-11.3 esitetyllä tavalla.

Allekirjoitettu ContentType-attribuutti PITÄÄ ilmoittaa ja se sisältää id-data-sisältötyypin (http://tools.ietf.org/html/rfc5652#section-4), kun sisältötyyppi on tarkoitettu viittaamaan satunnaisiin oktettijonoihin, kuten UTF-8-tekstiin tai ZIP-pakettiin, jolla on MimeType-alielementti.

Jos jäsenvaltion käyttämät allekirjoitukset perustuvat hyväksyttyyn varmenteeseen, allekirjoituksiin sisältyvät PKI-objektit (varmenneketjut, sulkutiedot, aikaleimat) ovat todennettavissa päätöksen 2009/767/EY mukaisesti käyttäen sen maan ”luotettavaa luetteloa”, joka vastaa allekirjoittajan varmenteen myöntäneen varmennepalvelujen tarjoajan valvonnasta tai akkreditoinnista.

([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]) Viimeisin versio on D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), päivätty 30.3.2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Taulukko 2

CAdES - BES (EPES)		**Yhteiset vähimmäisvaatimukset**
(ETSI TS 101 733, seuraavilla kuvatuilla elementeillä)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
P=Pakollinen; V=Vapaaehtoinen; S=Suositeltu; E=Ei käytössä		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	P	**Algoritmit:** sovellettavan kansallisen lainsäädännön mukaisesti; ohjeistusta ETSI TS 102 176 -asiakirjassa ja lisäsuosituksia ECRYPT2 D.SPA.7 -raportissa.
encapContentInfo SEQUENCE {		
eContentType ContentType,	P	id-Data
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	P/E	Allekirjoitettu ContentType-attribuutti ilmoitetaan ja se sisältää id-data-sisältötyypin (http://tools.ietf.org/html/rfc5652#section-4), kun sisältötyyppi on tarkoitettu viittaamaan satunnaisiin oktettijonoihin, kuten UTF-8-tekstiin tai ZIP-pakettiin, jolla on MimeType-alielementti
-- External Data (if signature detached)*		Ellei irrallinen allekirjoitus muutoin luettavissa. * Ulkoisella datalla tarkoitetaan irrallisella allekirjoituksella suojattua dataa, joka ei sisälly CAdES-allekirjoituksen eContent-kenttään. Suosituksena on, että allekirjoitettu ulkoinen data sisällytetään ZIP-tiedostoon yhdessä allekirjoituksen kanssa.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	P	PITÄÄ sisältää allekirjoittajan X509-varmenne. On SUOSITELTAVAA, että tähän sisällytetään varmenteet koko varmenneketjusta luotettuun varmenteeseen (*trust anchor*) saakka.
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	V	
signerInfos SET OF	P	Vähintään yksi signerInfo-tieto.
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	V	(Suojaamaton arvo)
digestAlgorithm DigestAlgorithmIdentifier,	P	**Algoritmit:** sovellettavan kansallisen lainsäädännön mukaisesti; ohjeistusta ETSI TS 102 176 -asiakirjassa ja lisäsuosituksia ECRYPT2 D.SPA.7 -raportissa.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	P	
attrType OBJECT IDENTIFIER,	P/V	**PITÄÄ olla:** id-contentType (with id data) id-messageDigest id-aa-ets-signingCertificateV2 or id-aa-signingCertificate PITÄÄ olla: signingTime **VAPAAEHTOINEN:** id-aa-ets-sigPolicyId Muut vapaaehtoiset attribuutit asiakirjan ETSI TS 101 733 mukaisesti.
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmit:** sovellettavan kansallisen lainsäädännön mukaisesti; ohjeistusta ETSI TS 102 176 -asiakirjassa ja lisäsuosituksia ECRYPT2 D.SPA.7 -raportissa.
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	V	

SEQUENCE {
attrType OBJECT IDENTIFIER,
attrValues SET OF
AttributeValue
} OPTIONAL
}
}
	V	

OSIO 3 – PAdES-PART 3 (BES/EPES):

Allekirjoituksen PITÄÄ käyttää PAdES-BES- (tai PAdES-EPES-) -allekirjoituslaajennusta, siten kuin ne on määritelty PAdES-Part3-eritelmissä asiakirjassa ETSI TS 102 778 ([1]), ja se vastaa seuraavia lisäeritelmiä:

Tiivisteen laskemiseen EI SAA käyttää MD5-algoritmia (RFC 1321). Allekirjoittajia kehotetaan tutustumaan sovellettaviin kansallisiin lakeihin ja ohjeistojen osalta asiakirjaan ETSI TS 102 176 ([2]) sekä ECRYPT2 D.SPA.x -raporttiin ([3]), joka sisältää lisää suosituksia sähköisissä allekirjoituksissa hyväksyttävistä algoritmeista ja parametreista.

Allekirjoitettujen attribuuttien PITÄÄ sisältää viittaus allekirjoittajan digitaaliseen X.509 v3 -varmenteeseen (RFC 5035) ja *SignedData.certificates*-kentän PITÄÄ sisältää sen arvo.

([1]) ETSI TS 102 778–3 v1.2.1.: PDF Advanced Signatures (PAdES), PAdES Enhanched–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]) Viimeisin versio on D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010), päivätty 30.3.2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Allekirjoittamisajankohta ilmoitetaan allekirjoitussanastoon kuuluvan **M**-tietueen arvona.

Jos jäsenvaltion käyttämät allekirjoitukset perustuvat hyväksyttyyn varmenteeseen, allekirjoituksiin sisältyvät PKI-objektit (varmenneketjut, sulkutiedot, aikaleimat) ovat todennettavissa päätöksen 2009/767/EY mukaisesti käyttäen sen maan ”luotettavaa luetteloa”, joka vastaa allekirjoittajan varmenteen myöntäneen varmennepalvelujen tarjoajan valvonnasta tai akkreditoinnista.