DEĊIŻJONIJIET

DEĊIŻJONI TAL-KUMMISSJONI

tal-25 ta' Frar 2011

li tistabbilixxi rekwiżiti minimi għall-ipproċessar transkonfinali ta' dokumenti ffirmati elettronikament minn awtoritajiet kompetenti skont id-Direttiva 2006/123/KE tal-Parlament Ewropew u tal-Kunsill dwar is-servizzi fis-suq intern

(notifikata bid-dokument numru C(2011) 1081)

(Test b'relevanza għaż-ŻEE)

(2011/130/UE)

IL-KUMMISSJONI EWROPEA,

Wara li kkunsidrat it-Trattat dwar il-Funzjonament tal-Unjoni Ewropea,

Wara li kkunsidrat id-Direttiva 2006/123/KE tal-Parlament Ewropew u tal-Kunsill tat-12 ta' Diċembru 2006 dwar is-servizzi fis-suq intern [1], u b'mod partikolari l-Artikolu 8(3) tagħha,

Billi:

(1) Il-fornituri tas-servizzi li s-servizzi tagħhom jaqgħu fl-ambitu tad-Direttiva 2006/123/KE għandhom jkunu kapaċi jtemmu, permezz tal-Punti ta' Kuntatt Waħdieni u permezz ta' mezzi elettroniċi, il-proċeduri u l-formalitajiet meħtieġa għall-aċċess għal u l-eżerċizzju tal-attivitajiet tagħhom. Fil-limiti stabbiliti fl-Artikolu 5(3) tad-Direttiva 2006/123/KE, xorta jista' jkun hemm każijiet fejn il-fornituri tas-servizzi jkollhom jissottmettu dokumenti oriġinali, kopji awtentikati jew traduzzjonijiet awtentikati meta jtemmu dawn il-proċeduri u formalitajiet. F'dawk il-każijiet, il-fornituri tas-servizzi jistgħu jkunu meħtieġa li jissottmettu dokumenti ffirmati elettronikament minn awtoritajiet kompetenti.

(2) L-użu transkonfinali ta' firem elettroniċi avvanzati sostnuti minn ċertifikat ikkwalifikat huwa ffaċilitat permezz tad-Deċiżjoni tal-Kummissjoni 2009/767/KE tas-16 ta' Ottubru 2009 li tistipula miżuri li jiffaċilitaw l-użu ta' proċeduri b'mezzi elettroniċi permezz tal-"punti ta' kuntatt waħdieni" skont id-Direttiva 2006/123/KE tal-Parlament Ewropew u tal-Kunsill dwar is-servizzi fis-suq intern [2] li, *inter alia*, timponi obbligu fuq l-Istati Membri sabiex iwettqu valutazzjonijiet tar-riskju qabel ma jeħtieġu dawn il-firem elettroniċi mill-fornituri tas-servizzi u tistabbilixxi regoli għall-aċċettazzjoni mill-Istati Membri ta' firem elettroniċi avvanzati bbażati fuq ċertifikati kwalifikati, maħluqa kemm bl-użu ta' tagħmir għall-ħolqien tal-firem siguri kif ukoll mingħajru. Madankollu, id-Deċiżjoni 2009/767/KE ma tittrattax il-formati ta' firem elettroniċi f'dokumenti maħruġa minn awtoritajiet kompetenti, li jeħtieġ li jiġu sottomessi mill-fornituri tas-servizz meta jtemmu l-proċeduri u l-formalitajiet rilevanti.

(3) Minħabba li l-awtoritajiet kompetenti fl-Istati Membri attwalment jużaw formati differenti ta' firem elettroniċi avvanzati sabiex jiffirmaw id-dokumenti tagħhom elettronikament, l-Istati Membru riċevituri li jkollhom jipproċessaw dawn id-dokumenti jistgħu jħabbtu wiċċhom ma' diffikultajiet tekniċi minħabba l-varjetà ta' formati ta' firem użati. Sabiex jippermettu lill-fornituri tas-servizzi jtemmu l-proċeduri tagħhom u l-formalitajiet bejn il-fruntieri permezz ta' mezzi elettroniċi, huwa meħtieġ li jiġi żgurat li mill-inqas numru ta' formati ta' firem elettroniċi avvanzati jkunu jistgħu jiġu appoġġjati teknikament mill-Istati Membri meta jirċievu d-dokumenti ffirmati elettronikament minn awtoritajiet kompetenti ta' Stati Membri oħra. Id-definizzjoni ta' għadd ta' formati ta' firem elettroniċi avvanzati li jeħtieġ li jkunu appoġġjati teknikament mill-Istat Membru riċevituri tippermetti awtomizzazzjoni akbar u ttejjeb l-interoperabbiltà transfruntiera tal-proċeduri elettroniċi.

(4) L-Istati Membri li l-awtoritajiet kompetenti tagħhom jużaw formati ta' firem elettroniċi li huma differenti minn dawk sostnuti b'mod komuni, jistgħu jkunu implimentaw metodi ta' validazzjoni li jippermettu li l-firem tagħhom li jiġu vverifikati wkoll bejn il-fruntieri. Meta dan ikun il-każ u sabiex l-Istati Membri riċevituri jkunu jistgħu jiddependu fuq dawn l-għodod ta' validazzjoni, huwa meħtieġ li l-informazzjoni dwar dawn l-għodod tkun disponibbli b'mod aċċessibbli faċilment sakemm l-informazzjoni meħtieġa ma tkunx inkluża direttament fid-dokumenti elettroniċi, fil-firem elettroniċi jew fil-mezzi portabbli tad-dokumenti elettroniċi.

(5) Din id-Deċiżjoni ma taffettwax id-determinazzjoni mill-Istati Membri ta' x'jikkostitwixxi dokument oriġinali, kopja awtentikata jew traduzzjoni awtentikata. L-għan tagħha huwa limitat biex tiffaċilita l-verifika ta' firem elettroniċi jekk dawn ikunu użati fid-dokumenti oriġinali, kopji awtentikati jew traduzzjonijiet awtentikati li l-fornituri tas-servizzi jistgħu jeħtieġu li jissottomettu permezz tal-Punti ta' Kuntatt Waħdieni.

[1] ĠU L 376, 27.12.2006, p. 36.
[2] ĠU L 274, 20.10.2009, p. 36.

(6) Sabiex l-Istati Membri jkunu awtorizzati jimplimentaw l-għodod tekniċi meħtieġa, huwa xieraq li din id-Deċiżjoni tapplika mill-1 ta' Awwissu 2011.

(7) Il-miżuri stabbiliti f'din id-Deċiżjoni huma skont l-opinjoni tal-Kumitat tad-Direttiva tas-Servizzi,

ADOTTAT DIN ID-DEĊIŻJONI:

Artikolu 1

Format ta' referenza għall-firem elettroniċi

1. L-Istati Membri għandhom idaħħlu fis-seħħ il-mezzi tekniċi meħtieġa li jippermettulhom jipproċessaw id-dokumenti ffirmati elettronikament li l-fornituri tas-servizzi jissottomettu fil-kuntest ta' kif jitlestew il-proċeduri u l-formalitajiet permezz tal-Punti ta' Kuntatt Waħdieni kif stabbilit fl-Artikolu 8 tad-Direttiva 2006/123/KE, u li huma ffirmati mill-awtoritajiet kompetenti ta' Stati Membri oħra b'firma elettronika avvanzata tal-XML jew CMS jew PDF fil-format BES jew EPES, li tikkonforma mal-ispeċifikazzjonijiet tekniċi stipulati fl-Anness.

2. L-Istati Membri li l-awtoritajiet kompetenti tagħhom jiffirmaw id-dokumenti msemmija fil-paragrafu 1 li jużaw formati oħra ta' firem elettroniċi minn dawk imsemmija fl-istess paragrafu, għandhom jinnotifikaw lill-Kummissjoni rigward possibbiltajiet eżistenti ta' validazzjoni li jippermettu lil Stati Membri oħra jivvalidaw il-firem elettroniċi irċevuti onlajn, mingħajr ħlas u b'mod li jinftiehem minn kelliema mhux nattivi sakemm l-informazzjoni meħtieġa ma tkunx diġà inkluża fid-dokument, fil-firma elettronika jew fit-trasportatur tad-dokument elettroniku. Il-Kummissjoni sejra tagħmel dik l-informazzjoni disponibbli għall-Istati Membri kollha.

Artikolu 2

Applikazzjoni

Din id-Deċiżjoni għandha tapplika mill-1 ta' Awwissu 2011.

Artikolu 3

Destinatarji

Din id-Deċiżjoni hija indirizzata lejn l-Istati Membri.

Magħmul fi Brussell, il-25 ta' Frar 2011.

Għall-Kummissjoni
Michel BARNIER
Membru tal-Kummissjoni

ANNESS

Speċifikazzjonijiet sabiex firma elettronika avvanzata XML, CMS jew PDF tkun sostnuta teknikament mill-istat membru riċevitur

Fil-parti tad-dokument li ġejja, il-kliem kjavi 'IRID' (MUST), 'MA JRIDX' (MUST NOT), 'MEĦTIEĠ' (REQUIRED), 'GĦANDU' (SHALL), 'MA GĦANDUX' (SHALL NOT), 'IMISSU' (SHOULD), 'MA JMISSUX' (SHOULD NOT), 'RAKKOMANDAT' (RECOMMENDED), 'JISTA' '(MAY)', u 'FAKULTATTIV' (OPTIONAL) għandhom jiġu interpretati kif deskritt fl-RFC 2119 ([1]).

TAQSIMA 1 – XAdES-BES/EPES:

Il-firma hija konformi mal-ispeċifikazzjonijiet tal-firem W3C XML ([2])

Il-firma TRID tkun forma ta' firma ta' mill-inqas XAdES-BES (jew EPES) kif speċifikat fl-ispeċifikazzjonijiet ETSI TS 101903 XAdES ([3]) u tikkonforma mal-ispeċifikazzjonijiet addizzjonali kollha li ġejjin:

Id-ds:CanonicalizationMethod li jispeċifika l-algoritmu tal-kanonikalizzazzjoni applikat għall-element SignedInfo qabel ma jitwettqu l-kalkoli tal-firma jidentifika wieħed mill-algoritmi li ġejjin biss:

Canonical XML 1.0 (iħalli barra l-kummenti): http://www.w3.org/TR/2001/REC-xml-c14n-20010315

Canonical XML 1.1 (iħalli barra l-kummenti): http://www.w3.org/2006/12/xml-c14n11

Canonicalization XML esklussiv 1.0 (iħalli barra l-kummenti): http://www.w3.org/2001/10/xml-exc-c14n#

Algoritmi oħra jew verżjonijet 'Bil-kummenti' ta' dawk elenkati hawn fuq MA JMISSHOMX jintużaw għall-ħolqien tal-firem iżda JMISSHOM ikunu sostnuti għal interoperabbiltà residwa għall-verifika tal-firem.

MD5 (RFC 1321) MA JRIDX jintuża bħala algoritmu diġeritur. Il-firmatarji jiġu referuti għal-liġijiet nazzjonali applikabbli, u għall-finijiet ta' linji gwida għall-ETSI TS 102176 ([4]) u għar-rapport ENCRYPT2 D.SPA.x ([5]) għal rakkomandazzjonijiet ulterjuri dwar algoritmi u parametri eliġibbli għall-firem elettroniċi.

L-użu ta' *trasformazzjonijiet* (transforms) huwa limitat għal dawk elenkati hawn taħt:

Trasformazzjonijiet tal-kanonikalizzazzjoni: ara l-ispeċifikazzjonijiet relatati ta' hawn fuq;

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

Filtrazzjoni:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): għal raġunijiet ta' kumpatibbiltà u konformità mal-XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): bħala suċċessur għal XPath minħabba kwistjonijiet relatati mar-rendiment

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

XSLT (style sheet) **transform**.

Id-ds:KeyInfo element IRID jinkludi ċ-ċertifikat diġitali X.509 v3 tal-firmatarju (jiġifieri l-valur tiegħu u mhux biss referenza għalih);

Il-proprjetà tal-firma ffirmata bis-'SigningCertificate' TRID tinkludi il-valur diġeritur (CertDigest) u l-IssuerSerial taċ-ċertifikat tal-firmatarju maħżun fid-ds:KeyInfo u l-URI fakultattiv fil-qasam tas-'SigningCertificate' MA JRIDX jintuża;

Il-proprjetà tal-firma ffirmata permezz tas-SigningTime hija preżenti u tinkludi l-UTC espress bħala xsd:dateTime (http://www.w3.org/TR/xmlschema-2/# dateTime);

L-element DataObjectFormat IRID jkun preżenti u jkun fih sottoelement MimeType;

F'każ li l-firem użati mill-Istati Membri jkunu bbażati fuq ċertifikat awtentikat, l-oġġetti PKI (sensiliet ta' ċertifikati, dejta ta' revoka, timbrar tal-ħin (time-stamps)) li jkunu inklużi fil-firem huma verifikabbli permezz tal-Lista ta' Fiduċja, skont id-Deċiżjoni 2009/767/KE, tal-Istat Membru li jkun qed jissorvelja jew jakkredita s-CSP li ħareġ iċ-ċertifikat tal-firmatarju.

It-Tabella 1 tiġbor fil-qosor l-ispeċifikazzjonijiet li firma XAdES-BES/EPES trid tikkonforma magħhom sabiex tkun teknikament sostnuta mill-Istat Membru riċevitur.

([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 102176: 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 device".

([5]) L-iktar verżjoni riċenti hija D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), tat-30 ta' Marzu 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabella 1

XAdES - BES (EPES)		Rekwiżiti Minimi Komuni
(ETSI TS 103 903 japplika għall-elementi ta' profil li ġejjin)		
M=Mandatorju; O=Opzjonali; R=Rakkomandat; N=Nonutilizzat		
ds: Signature ID	M	
ds: SignedInfo	M	
ds: CanonicalizationMethod	M	*L-algoritmi kollha li ġejjin IRIDU jkunu appoġġjati għall-verifika tal-firma, il-ħolqien IMISSU jkun ristrett għal waħda minn dawn:* *- 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* *Metodi oħrajn jew verżjonijiet b'"#WithComments" tal-metodi ta' hawn fuq MA JMISSHOMX jintużaw.*
ds: SignatureMethod	M	***Algoritmi:*** *jirreferu għal-liġijiet nazzjonali applikabbli u għall-finijiet ta' linji gwida għal ETSI TS 102 176 u għar-rapport ECRYPT2 D.SPA.7 għal aktar rakkomandazzjonijiet.*
ds: Reference URI	M	Referenza waħda għal kull oġġett ta' dejta oriġinali li għandu jiġi ffirmat (URIs jistgħu jillinkjaw għal oġġett estern ukoll), + referenza għal element ta' SignedProperties
ds: Transforms	O	*Applikazzjonijiet li jivverifikaw IRIDU jappoġġjaw it-transformazzjonijiet kollha li ġejjin filwaqt li l-applikazzjoni tal-ħolqien tal-firma JMISSHA tirrestrinġi l-użu ta' dawk it-transformazzjonijiet għal dawn li ġejjin:* *- Transformazzjonijiet ta' kanonikalizzazzjoni: ara fuq* *- Kodifikar Base64* *- XPath u XPath Filter 2.0* *- Enveloped signature transform* *- XSLT transforms*
ds: DigestMethod	M	***Algoritmi:*** *irreferi għal-liġijiet nazzjonali applikabbli u għal għanijiet ta' linji gwida għal ETSI TS 102 176 u għar-rapport ECRYPT2 D.SPA.7 għal aktar rakkomandazzjonijiet.*
ds: DigestValue	M	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	M	
ds: KeyInfo	M	IRID ikollu ċertifikat X509 (proprjetà tal-firma SigningCertificate IRID jkun fiha il-valur tad-digeritur taċ-ċertifikat tal-firmatarju) Sensiela ta' ċertifikazzjoni ta' ċertifikat ta' firmatarju huma RRAKKOMANDATI li jiġu pprovduti bħala suġġeriment għall-iffaċilitar tal-proċess ta' validazzjoni (f'dan il-każ IRID jiġu pprovduti ċertifikati X.509).
ds: Object		
QualifyingProperties	M	
SignedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC (xsd: dateTime).
SigningCertificate	M	IRID ikun fih il-valur diġeritur taċ-ċertifikat tal-firmatarju maħżun fi ds:KeyInfo u URI fakultattiv huwa maqbuż (L-applikazzjonijiet JISTGĦU ifittxu/isibu ċ-ċertifikat tal-firmatarju fi ds:KeyInfo dwar il-bażi tal-ekwivalenza tal-hash).
SignaturePolicyIdentifier	O	għal forma EPES biss (u għal 'upper forms' mibnija fuq forom EPES)
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	M	Meta jintuża dan il-qasam, l-applikazzjonijiet GĦANDHOM jiżguraw li l-oġġetti tad-dejta jintwerew lill-utent bix-xieraq. Meta użat, IRID jintuża sottoelement MimeType.
CommitmentTypeIndication	O	
AllDataObjectsTimeStamp	O	
IndividualDataObjectTimeStamp	O	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	O	
UnsignedSignatureProperties		
CounterSignature	O	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Topoloġija tal-firma - Fajls oriġinali u firem tal-ippakkjar iffirmat		
SignatureEnveloped		Kollha JRIDU jkunu appoġġjati
SignatureEnveloping		
SignatureDetached		

TAQSIMA 2 – CAdES-BES/EPES:

Il-firma hija konformi mal-ispeċifikazzjonijiet tal-Firem Cryptographic Message Syntax (CMS) ([1])

Il-firma tuża attributi tal-firem ta' CAdES-BES (jew -EPES) kif speċifikat fl-ispeċifikazzjonijiet ETSI TS 101733 CAdES ([2]) u tikkonforma mal-ispeċifikazzjonijiet addizzjonali kif indikat fit-Tabella 2 ta' hawn taħt.

L-attribwiti kollha tal-CAdES li huma inklużi fil-kalkolu tat-timbrar tal-ħin tal-arikvjar (archive timestamp hash calculation) (ETSI TS 101733 V1.8.1 Anness K) IRID ikunu bil-kodifikazzjoni DER u kwalunkwe oħrajn jisgħtu jkunu bil-BER sabiex jissimplifikaw l-ipproċessar b'perkors wieħed tal-CAdES.

MD5 (RFC 1321) MA JRIDX jintuża bħala algoritmu diġeritur. Il-firmatarji jiġu riferuti għal-liġijiet nazzjonali applikabbli, u għall-finijiet ta' linji gwida għall-ETSI TS 102176 ([3]) u għar-rapport ENCRYPT2 D.SPA.x ([4]) għal rakkomandazzjonijiet ulterjuri dwar algoritmi u l-parametri eliġibbli għall-firem elettroniċi.

L-attributi ffirmati JRIDU jinkludu referenza għaċ-ċertifikat diġitali X.509 v3 tal-firmatarju (RFC 5035) u l-qasam *SignedData.certificates* IRID jinkludi l-valur tiegħu;

L-attribut iffirmat SigningTime IRID ikun preżenti u IRID jinkludi l-UTC espress bħala http://tools.ietf.org/html/rfc5652#section-11.3;

L-attribwut iffirmat ContentType IRID ikun preżenti u jinkludi id-data (http://tools.ietf.org/html/rfc5652#section-4) fejn it-tip tal-kontenut tad-dejta huwa maħsub li jirreferi għal sensiliet ta' ottetti arbitrarji, bħal test UTF-8 jew kontenitur ZIP b'sottoelement Mimetype;

F'każ li l-firem użati mill-Istati Membri jkunu bbażati fuq ċertifikat kwalifikat, l-oġġetti PKI (sensiliet ta' ċertifikati, dejta ta' revoka, timbrar tal-ħin) li huma inklużi fil-firem ikunu verifikabbli permezz tal-Lista ta' Fiduċja, skont id-Deċiżjoni tal-Kummissjoni 2009/767/KE, tal-Istat Membru li jkun qed jissorvelja jew jakkredita s-CSP li jkun ħareġ iċ-ċertifikat tal-firmatarju.

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

([4]) L-iktar verżjoni riċenti hija D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), tat-30 ta' Marzu 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabella 2

CAdES - BES (EPES)		**Rekwiżiti Minimi Komuni**
(ETSI TS 101 733 japplika għall-elementi ta' profil li ġejjin)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
M=Mandatorju; O=Opzjonali; R=Rakkomandat; N=Nonutilizzat		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	M	**Algoritmi: irreferi għal-liġijiet nazzjonali applikabbli u għall-finijiet tal-linji gwida għal ETSI TS 102 176 u għar-rapport ECRYPT2 D.SPA.7 għal aktar rakkomandazzjonijiet.**
encapContentInfo SEQUENCE {		
eContentType ContentType,	M	**id-Data**
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- mhux preżenti jekk firma distakkata },	M/N	**L-attribut iffirmat ContentType huwa preżenti u fih id-data (http://tools.ietf.org/html/rfc5652#section-4) fejn it-tip ta' kontenut tad-dejta huwa maħsub sabiex jirreferi għal sensiliet ottetti arbitrarji, bħal test UTF-8 jew kontenitur ZIP b'sottoelement MimeType**
-- Dejta esterna (jekk firma distakkata)*		**jekk firma 'detached' ma tkunx preżenti mod ieħor. * Dejta esterna tfisser dejta protetta b'firma distakkata li mhijiex inkluża fl-eContent tal-firma CAdES. Huwa rrakkomandat li tiġi inkluża dejta esterna ffirmata flimkien mal-firma fil-fajl ZIP.**
certificates [0] IMPLICIT CertificateSet OPTIONAL,	M	**IRID ikun fih ċertifikat X509 mingħand il-firmatarju. Hija RRAKKOMANDATA l-inklużjoni ta' Ċertifikati mis-sensiela ta' ċertifikazzjoni kollha sa 'trust anchor'.**
crls [1] RevocationInfoChoices IMPLICIT OPTIONAL,	O	
signerInfos SET OF	M	**Tal-anqas signerInfo wieħed**
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	O	**(Valur mhux protett)**
digestAlgorithm DigestAlgorithmIdentifier,	M	**Algoritmi: irreferi għal-liġijiet nazzjonali applikabbli u għall-finijiet tal-linji gwida għal ETSI TS 102 176 u għar-rapport ECRYPT2 D.SPA.7 għal aktar rakkomandazzjonijiet.**
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	M	
attrType OBJECT IDENTIFIER,	M/O	**IRID: id-contentType (bi id data) id-messageDigest id-aa-ets-signingCertificateV2 or id-aa-signingCertificate IRID: signingTime OPZJONALI: id-aa-ets-sigPolicyId Attributi opzjonali oħrajn kif iddefiniti f'ETSI TS 101 733.**
attrValues SET OF AttributeValue } FAKULTATTIV,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmi: irreferi għal-liġijiet nazzjonali applikabbli u għall-finijiet tal-linji gwida għal ETSI TS 102 176 u għar-rapport ECRYPT2 D.SPA.7 għal aktar rakkomandazzjonijiet.**
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	O	

SEQUENCE {
attrType OBJECT IDENTIFIER,
attrValues SET OF
AttributeValue
} FAKULTATTIV
}
}
	O	

TAQSIMA 3 – PAdES-PART 3 (BES/EPES):

Il-firma TRID tuża *signature extension* PAdES-BES (jew -EPES) kif speċifikat fl-ispeċifikazzjonijiet ETSI TS 102778 PAdES-Part3 ([1]) u tikkonforma mal-ispeċifikazzjonijiet addizzjonali li ġejjin:

MD5 (RFC 1321) MA JRIDX jintuża bħala algoritmu diġeritur. Il-firmatarji jiġu rriferuti għal-liġijiet nazzjonali applikabbli, u għall-finijiet ta' linji gwida, għall-ETSI TS 102176 ([2]) u għar-rapport ENCRYPT2 D.SPA.x ([3]) għal rakkomandazzjonijiet ulterjuri dwar algoritmi u parametri eliġibbli għall-firem elettroniċi.

L-attributi ffirmati JRIDU jinkludu referenza għaċ-ċertifikat diġitali X.509 v3 tal-firmatarju (RFC 5035) u l-qasam tas-*SignedData.certificates* IRID jinkludi l-valur tiegħu;

([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]) L-iktar verżjoni riċenti hija D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), tat-30 ta' Marzu 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Il-ħin tal-iffirmar huwa indikat permezz tal-valur tal-entratura **M** fid-dizzjunarju tal-firem;

F'każ li l-firem użati mill-Istati Membri jkunu bbażati fuq ċertifikat ikkwalifikat, l-oġġetti PKI (sensiliet ta' ċertifikati, dejta ta' revoka, timbrar tal-ħin) li jkunu inklużi fil-firem huma verifikabbli permezz tal-Lista ta' Fiduċja, skont id-Deċiżjoni 2009/767/KE, tal-Istat Membru li jkun qed jissorvelja jew jakkredita s-CSP li jkun ħareġ iċ-ċertifikat tal-firmatarju.