DECISIONI

DECISIONE DELLA COMMISSIONE

del 25 febbraio 2011

che istituisce requisiti minimi per il trattamento transfrontaliero dei documenti firmati elettronicamente dalle autorità competenti a norma della direttiva 2006/123/CE del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno

[notificata con il numero C(2011) 1081]

(Testo rilevante ai fini del SEE)

(2011/130/UE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno [1], in particolare l'articolo 8, paragrafo 3,

considerando quanto segue:

(1) I prestatori di servizi che rientrano nell'ambito di applicazione della direttiva 2006/123/CE devono poter espletare, tramite gli sportelli unici e per via elettronica, le procedure e le formalità necessarie per accedere alle loro attività ed esercitarle. Entro i limiti stabiliti all'articolo 5, paragrafo 3, della direttiva 2006/123/CE, vi possono tuttora essere casi in cui i prestatori di servizi debbono presentare documenti originali, copie certificate o traduzioni autenticate ai fini dell'espletamento di tali procedure e formalità. In tali casi i prestatori di servizi potrebbero dover presentare documenti firmati elettronicamente dalle autorità competenti.

(2) L'uso transfrontaliero di firme elettroniche avanzate basate su un certificato qualificato è agevolato dalla decisione 2009/767/CE della Commissione, del 16 ottobre 2009, che stabilisce misure per facilitare l'uso di procedure per via elettronica mediante gli «sportelli unici» di cui alla direttiva 2006/123/CE del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno [2] che tra l'altro impone agli Stati membri l'obbligo di effettuare valutazioni del rischio prima di richiedere tali firme elettroniche ai prestatori di servizi e stabilisce regole per l'accettazione da parte degli Stati membri di firme elettroniche avanzate basate su un certificato qualificato, con o senza dispositivo per la creazione di una firma sicura. La decisione 2009/767/CE non tratta tuttavia dei formati delle firme elettroniche nei documenti emessi dalle autorità competenti, che devono essere presentati dai prestatori di servizi in sede di espletamento delle procedure e formalità pertinenti.

(3) Poiché le autorità competenti degli Stati membri utilizzano attualmente diversi formati di firme elettroniche avanzate per firmare i loro documenti elettronicamente, gli Stati membri riceventi che devono trattare tali documenti potrebbero incorrere in difficoltà tecniche a causa della varietà di formati di firma utilizzati. Per consentire ai prestatori di servizi di espletare le loro procedure e formalità a livello transfrontaliero tramite mezzi elettronici, è necessario garantire che almeno una serie di formati di firma elettronica avanzata possano essere supportati tecnicamente dagli Stati membri quando questi ricevono documenti firmati elettronicamente dalle autorità competenti di altri Stati membri. La definizione di una serie di formati di firma elettronica avanzata che devono essere supportati tecnicamente dallo Stato membro ricevente consentirebbe una maggiore automazione e migliorerebbe l'interoperabilità transfrontaliera delle procedure elettroniche.

(4) Gli Stati membri le cui autorità competenti utilizzano altri formati di firma elettronica rispetto a quelli supportati comunemente potrebbero aver applicato mezzi di convalida che consentono di verificare le loro firme anche a livello transfrontaliero. In questo caso, onde far sì che gli Stati membri riceventi possano fare affidamento su tali mezzi di convalida, è necessario mettere a disposizione informazioni facilmente accessibili in proposito, a meno che le informazioni necessarie non siano incluse direttamente nei documenti elettronici, nelle firme elettroniche o nei supporti dei documenti elettronici.

(5) La presente decisione non influisce sulla definizione di originale, copia certificata o traduzione autenticata da parte degli Stati membri. Ha solo l'obiettivo di agevolare la verifica delle firme elettroniche utilizzate negli originali, nelle copie certificate o nelle traduzioni autenticate presentate dai prestatori di servizi tramite gli sportelli unici.

[1] GU L 376 del 27.12.2006, pag. 36.
[2] GU L 274 del 20.10.2009, pag. 36.

(6) Per consentire agli Stati membri di applicare gli strumenti tecnici necessari, è opportuno che la presente decisione si applichi a partire dal 1º agosto 2011.

(7) Le misure di cui alla presente decisione sono conformi al parere del comitato della direttiva servizi,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Formato di riferimento per le firme elettroniche

1. Gli Stati membri si dotano degli strumenti tecnici necessari che consentono loro di trattare i documenti presentati dai prestatori di servizi, ai fini dell'espletamento delle procedure e delle formalità tramite gli sportelli unici di cui all'articolo 8 della direttiva 2006/123/CE, che sono firmati elettronicamente dalle autorità competenti di altri Stati membri con una firma elettronica avanzata XML, CMS o PDF in formato BES o EPES che rispetti le specifiche tecniche riportate nell'allegato.

2. Gli Stati membri le cui autorità competenti firmano i documenti di cui al paragrafo 1 utilizzando formati di firma elettronica diversi da quelli indicati in tale paragrafo notificano alla Commissione le possibilità di convalida esistenti che consentono agli altri Stati membri di convalidare le firme elettroniche ricevute on line, gratuitamente e in modo comprensibile per i non madre lingua a meno che le informazioni richieste non siano già incluse nel documento, nella firma elettronica o nel supporto del documento elettronico. La Commissione mette tali informazioni a disposizione di tutti gli Stati membri.

Articolo 2

Applicazione

La presente decisione si applica a decorrere dal 1º agosto 2011.

Articolo 3

Destinatari

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 25 febbraio 2011.

Per la Commissione
Michel BARNIER
Membro della Commissione

ALLEGATO

Specifiche per una firma elettronica avanzata XML, CMS o PDF che lo Stato membro ricevente deve supportare tecnicamente

Nella parte seguente del documento le parole chiave «DEVE» (*MUST*/*SHALL*), «NON DEVE» (*MUST NOT*/*SHALL NOT*), «È RICHIESTO» (*REQUIRED*), «DOVREBBE» (*SHOULD*), «NON DOVREBBE» (*SHOULD NOT*), «SI RACCOMANDA» (*RECOMMENDED*), «PUÒ/POTREBBE» (*MAY*), e «OPZIONALE» (*OPTIONAL*) devono essere interpretate nell'accezione di cui al documento RFC 2119 ([1]).

SEZIONE 1 — XAdES-BES/EPES

La firma è conforme alle specifiche W3C XML Signature ([2]).

La firma DEVE essere almeno di forma XAdES-BES (o -EPES) come indicato nelle specifiche ETSI TS 101 903 XAdES ([3]) e rispetta tutte le specifiche aggiuntive seguenti:

Il ds:CanonicalizationMethod che specifica l'algoritmo di canonicalizzazione applicato all'elemento SignedInfo prima dell'esecuzione dei calcoli della firma identifica solo uno dei seguenti algoritmi:

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

Altri algoritmi o versioni «Con commenti» degli algoritmi sopraelencati NON DOVREBBERO essere utilizzati per la creazione della firma ma DOVREBBERO essere supportati per interoperabilità residua per la verifica della firma.

L'MD5 (RFC 1321) NON DEVE essere utilizzato come algoritmo digest. I firmatari sono rinviati alle leggi nazionali applicabili e, per orientamenti, a ETSI TS 102 176 ([4]) e alla relazione ECRYPT2 D.SPA.x ([5]) per maggiori raccomandazioni sugli algoritmi e sui parametri ammissibili per le firme elettroniche.

L'uso di *transform* è limitato a quelli seguenti:

Transform di canonicalizzazione: cfr. le relative specifiche di cui sopra

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

Filtraggio:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): per ragioni di compatibilità e conformità a XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): come successore di Xpath a causa di problemi di performance

Transform di firma con metodo Enveloped: (http://www.w3.org/2000/09/xmldsig#enveloped-signature)

Transform XSLT (foglio di stile)

Il ds:KeyInfo element DEVE includere il certificato digitale X.509 v3 del firmatario (ovvero il suo valore e non solo un riferimento ad esso).

La proprietà «SigningCertificate» della firma firmata DEVE contenere il valore digest (CertDigest) e lo IssuerSerial del certificato del firmatario memorizzato in ds:KeyInfo e l'opzionale URI nel campo «SigningCertificate» NON DEVE essere utilizzato.

La proprietà SigningTime della firma firmata è presente e contiene l'UTC espresso come xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

L'elemento DataObjectFormat DEVE ESSERE presente e contenere un sub-elemento MimeType.

Se le firme utilizzate dagli Stati membri sono basate su un certificato qualificato, gli oggetti del PKI (catene certificato, dati revoca, *time-stamp*) che sono inclusi nelle firme sono verificabili utilizzando l'elenco di fiducia, conformemente alla decisione 2009/767/CE, dello Stato membro che vigila o accredita il CSP che ha emesso il certificato del firmatario.

La tabella 1 sintetizza le specifiche che una firma XAdES-BES/EPES deve soddisfare per essere supportata tecnicamente dallo Stato membro ricevente.

([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; parte 1: Hash functions and asymmetric algorithms; parte 2: «Secure channel protocols and algorithms for signature creation devices».
([5]) L'ultima versione è D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), dated 30 March 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabella 1

XAdES — BES (EPES)		**Requisiti minimi comuni**
(ETSI TS 103 903 si applica con i seguenti elementi profilati)		
M = Obbligatorio; O = Opzionale; R = Raccomandato; N = Non usato		
ds: Signature ID	M	
ds: SignedInfo	M	
ds: CanonicalizationMethod	M	*Tutti i seguenti algoritmi DEVONO essere supportati per la verifica della firma, la creazione DOVREBBE limitarsi ad uno di questi metodi:* *- 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* *NON DOVREBBERO essere utilizzati altri metodi o versioni "#Con commenti" dei suddetti metodi.*
ds: SignatureMethod	M	***Algoritmi:*** *si riferiscono alle leggi nazionali applicabili e a fini di orientamenti a ETSI TS 102 176 e alla relazione ECRYPT2 D.SPA.7 per ulteriori raccomandazioni.*
ds: Reference URI	M	Un riferimento ad ogni oggetto di dati originario da firmare (gli URI possono anche puntare ad un oggetto esterno), + riferimento all'elemento SignedProperties.
ds: Transforms	O	*Le applicazioni di verifica DEVONO sostenere tutti i seguenti transform mentre l'applicazione di creazione della firma DOVREBBE limitare l'uso di tali transform ai seguenti:* *- Transform di canonicalizzazione: cfr. supra* *- Codifica Base64* *- XPath e XPath Filter 2.0* *- Transform di firma con metodo Enveloped* *- Transform di XSLT*
ds: DigestMethod	M	***Algoritmi:*** *si riferiscono alle leggi nazionali applicabili e a fini di orientamento a ETSI TS 102 176 e alla relazione ECRYPT2 D.SPA.7 per ulteriori raccomandazioni.*
ds: DigestValue	M	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	M	
ds: KeyInfo	M	DEVE contenere un certificato X509 (la proprietà SigningCertificate firmata DEVE contenere il valore digest di questo certificato del firmatario). Si RACCOMANDA di fornire la catena di certificazione del certificato del firmatario per facilitare il processo di convalida (in questo caso DEVONO essere forniti i certificati X.509).
ds: Object		
QualifyingProperties	M	
SignedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC (xsd: dateTime).
SigningCertificate	M	DEVE contenere il valore di digest del certificato del firmatario memorizzato in ds:KeyInfo e l'URI opzionale è omesso (le applicazioni POSSONO cercare/trovare il certificato del firmatario in ds:KeyInfo sulla base dell'equivalenza dello hash).
SignaturePolicyIdentifier	O	Solo per la forma EPES (e per forme superiori costruite dalla forma EPES).
Signature ProductionPlace	O	
SignerRole	O	
/SignedSignatureProperties		
SignedDataObjectProperties	O	
DataObjectFormat	M	In caso di utilizzo di questo campo, le applicazioni DEVONO garantire che gli oggetti di dati siano indicati conseguentemente all'utente. In tal caso DEVE essere utilizzato un elemento figlio MimeType.
CommitmentTypeIndication	O	
AllDataObjectsTimeStamp	O	
IndividualDataObjectTimeStamp	O	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	O	
UnsignedSignatureProperties		
CounterSignature	O	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Signature topology — Packaging signed original files and signatures		
SignatureEnveloped		Tutti DEVONO essere supportati.
SignatureEnveloping		
SignatureDetached		

SEZIONE 2 — CAdES-BES/EPES

La firma è conforme alle specifiche della Cryptographic Message Syntax (CMS) Signature [1].

La firma utilizza gli attributi firma CAdES-BES (o -EPES) come indicato nelle specifiche ETSI TS 101 733 CAdES [2] e rispetta le specifiche aggiuntive come indicato sotto nella tabella 2.

Tutti gli attributi di CAdES che sono inclusi nel calcolo dello hash timestamp dell'archivio (ETSI TS 101 733 V1.8.1 allegato K) DEVONO essere in codice DER e tutti gli altri possono essere in BER per semplificare il trattamento one-pass di CAdES.

L'MD5 (RFC 1321) NON DEVE essere utilizzato come algoritmo digest. I firmatari sono rinviati alle leggi nazionali applicabili e, per orientamenti, a ETSI TS 102 176 [3] e alla relazione ECRYPT2 D.SPA.x [4] per maggiori raccomandazioni sugli algoritmi e sui parametri ammissibili per le firme elettroniche.

Gli attributi firmati DEVONO includere un riferimento al certificato digitale X.509 v3 del firmatario (RFC 5035) e il campo *SignedData.certificates* DEVE includere il suo valore.

L'attributo SigningTime firmato DEVE essere presente e DEVE contenere l'UTC espresso come in http://tools.ietf.org/html/rfc5652#section-11.3.

L'attributo ContentType firmato DEVE essere presente e contiene id-data (http://tools.ietf.org/html/rfc5652#section-4) dove il content type dei dati si riferisce a stringhe arbitrarie di otteti come il testo UTF-8 o il container ZIP con sub-elemento MimeType.

Se le firme utilizzate dagli Stati membri sono basate su un certificato qualificato, gli oggetti del PKI (catene certificato, dati revoca, *time-stamp*) che sono inclusi nelle firme sono verificabili utilizzando l'elenco di fiducia, conformemente alla decisione 2009/767/CE, dello Stato membro che vigila o accredita il CSP che ha emesso il certificato del firmatario.

---

[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; parte 1: Hash functions and asymmetric algorithms; parte 2: «Secure channel protocols and algorithms for signature creation devices».

[4] L'ultima versione è D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), dated 30 March 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Tabella 2

CAdES — BES (EPES)		**Requisiti minimi comuni**
(ETSI TS 101 733 si applica con i seguenti elementi profilati)		
ASN.1		
ContentInfo ::= SEQUENCE {		
contentType ContentType, -- id-signedData		
content [0] EXPLICIT ANY DEFINED BY contentType }		
M = Obbligatorio; O = Opzionale; R = Raccomandato; N = Non usato		
SignedData ::= SEQUENCE {		
version CMSVersion,		
digestAlgorithms DigestAlgorithmIdentifiers,	M	**Algoritmi**: si riferiscono alle leggi nazionali applicabili e a fini di orientamento a ETSI TS 102 176 e alla relazione ECRYPT2 D.SPA.7 per ulteriori raccomandazioni.
encapContentInfo SEQUENCE {		
eContentType ContentType,	M	id-Data
eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },	M/N	L'attributo ContentType firmato è presente e contiene id-data (http://tools.ietf.org/html/rfc5652#section-4) mentre il tipo data content si riferisce a stringhe arbitrarie di otteti come il testo UTF-8 o il container ZIP con sub-elemento MimeType.
-- External Data (if signature detached)*		Se la firma staccata non è altrimenti presente. * Dati esterni significa dati protetti da una firma staccata che non è inclusa nell'eContent della firma CAdES. Si raccomanda di includere nel file ZIP dati esterni firmati insieme alla firma.
certificates [0] IMPLICIT CertificateSet OPTIONAL,	M	DEVE contenere il certificato X509 del firmatario. È RACCOMANDATA l'inclusione di certificati dell'intera catena di certificazione fino ad un trust anchor.
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,	O	
signerInfos SET OF	M	Almeno un signerInfo.
SEQUENCE { -- SignerInfo		
version CMSVersion,		
sid SignerIdentifier,	O	(Valore non protetto)
digestAlgorithm DigestAlgorithmIdentifier,	M	**Algoritmi**: si riferiscono alle leggi nazionali applicabili e a fini di orientamento a ETSI TS 102 176 e alla relazione ECRYPT2 D.SPA.7 per ulteriori raccomandazioni.
signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF		
SEQUENCE { -- Attribute	M	
attrType OBJECT IDENTIFIER,	M/O	**OBBLIGATORIO**: id-contentType (con dati id) id-messageDigest id-aa-ets-signingCertificateV2 o id-aa-signingCertificate OBBLIGATORIO: signingTime **OPZIONALE**: id-aa-ets-sigPolicyId Altri attributi opzionali come definiti in ETSI TS 101 733.
attrValues SET OF AttributeValue } OPTIONAL,		
signatureAlgorithm SignatureAlgorithmIdentifier,		**Algoritmi**: si riferiscono alle leggi nazionali applicabili e per fini di orientamento a ETSI TS 102 176 e alla relazione ECRYPT2 D.SPA.7 per ulteriori raccomandazioni.
signature OCTET STRING, -- SignatureValue		
unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF	O	

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

SEZIONE 3 — PAdES-PARTE 3 (BES/EPES):

La firma DEVE utilizzare una estensione della firma PAdES-BES (o -EPES) come indicato nelle specifiche ETSI TS 102 778 PAdES-Part3 ([1]) e rispetta tutte le specifiche aggiuntive seguenti:

l'MD5 (RFC 1321) NON DEVE essere utilizzato come algoritmo digest. I firmatari sono rinviati alle leggi nazionali applicabili e, per orientamenti, a ETSI TS 102 176 ([2]) e alla relazione ECRYPT2 D.SPA.x ([3]) per maggiori raccomandazioni sugli algoritmi e sui parametri ammissibili per le firme elettroniche.

Gli attributi firmati DEVONO includere un riferimento al certificato digitale X.509 v3 del firmatario (RFC 5035) e il campo *SignedData.certificates* DEVE includere il suo valore.

([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; parte 1: Hash functions and asymmetric algorithms; parte 2: «Secure channel protocols and algorithms for signature creation devices».

([3]) L'ultima versione è D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), del 30 marzo 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Il momento della firma è indicato dal valore della voce (entry) M nel dizionario della firma.

Se le firme utilizzate dagli Stati membri sono basate su un certificato qualificato, gli oggetti del PKI (catene certificato, dati revoca, *time-stamp*) che sono inclusi nelle firme sono verificabili utilizzando l'elenco di fiducia, conformemente alla decisione 2009/767/CE, dello Stato membro che vigila o accredita il CSP che ha emesso il certificato del firmatario.