РЕШЕНИЯ

РЕШЕНИЕ НА КОМИСИЯТА

от 25 февруари 2011 година

за установяване на минимални изисквания за трансграничната обработка на документи, подписани електронно от компетентните органи съгласно Директива 2006/123/ЕО на Европейския парламент и на Съвета относно услугите на вътрешния пазар

(нотифицирано под номер C(2011) 1081)

(текст от значение за ЕИП)

(2011/130/ЕС)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Директива 2006/123/ЕО на Европейския парламент и на Съвета от 12 декември 2006 г. относно услугите на вътрешния пазар [1], и по-специално член 8, параграф 3 от нея,

като има предвид, че:

(1) Доставчиците на услуги, чиито услуги попадат в обхвата на Директива 2006/123/ЕО, трябва да могат да приключат процедурите и формалностите, необходими за започване и осъществяване на тяхната дейност, посредством единични звена за контакт или електронни средства. В рамките на ограниченията, посочени в член 5, параграф 3 от Директива 2006/123/ЕО, може да съществуват случаи, при които при изпълнението на тези процедури и формалности доставчиците на услуги трябва да представят оригинални документи, заверени копия или заверени преводи. В тези случаи на доставчиците на услуги може да се наложи да представят документи, подписани електронно от компетентните органи.

(2) Трансграничното използване на усъвършенствани електронни подписи на базата на квалифицирано удостоверение беше улеснено с Решение 2009/767/ЕО на Комисията от 16 октомври 2009 г. за определяне на мерки, улесняващи прилагането на процедури с помощта на електронни средства чрез „единичните звена за контакт“ в съответствие с Директива 2006/123/ЕО на Европейския парламент и на Съвета относно услугите на вътрешния пазар [2], което решение задължава държавите-членки да направят оценка на въздействието, преди да изискват въпросните електронни подписи от доставчиците на услуги, като в него също така се определят и правила за одобряването от държавите-членки на усъвършенствани електронни подписи на базата на квалифицирани удостоверения, създадени със или без помощта на устройство за създаване на защитени електронни подписи. В Решение 2009/767/ЕО обаче не са обхванати форматите на електронни подписи в издаваните от компетентните органи документи, които трябва да бъдат предоставени от доставчиците на услуги с оглед приключването на съответните процедури и формалности.

(3) Понастоящем за електронното подписване на своите документи компетентните органи в държавите-членки използват различни формати на усъвършенствани електронни подписи и следователно получаващите държави-членки, които трябва да обработят въпросните документи, могат да изпитат технически затруднения вследствие на използваните разнообразни формати на подписи. За да могат доставчиците на услуги да приключат процедурите и формалностите в трансграничен мащаб по електронен път, е необходимо в държавите-членки да се осигури техническа възможност за обработка поне на определен брой формати на усъвършенствани електронни подписи при получаването на документи, подписани електронно от компетентните органи на други държави-членки. Определянето на няколко формата на усъвършенствани електронни подписи, които трябва да бъдат технически поддържани от получаващата държава-членка, би увеличило автоматизацията и подобрило трансграничната оперативна съвместимост на електронните процедури.

(4) Възможно е държавите-членки, чиито компетентни органи използват други, по-рядко поддържани формати на електронни подписи, вече да са въвели средства за валидиране, които позволяват трансграничното валидиране на техните подписи. В такъв случай и с оглед получаващите държави-членки да могат да разчитат на тези инструменти за валидиране се налага информацията относно въпросните инструменти да бъде леснодостъпна, освен когато необходимата информация е включена непосредствено в електронните документи, в електронните подписи или в носителите на електронния документ.

(5) Настоящото решение не засяга направените от държавите-членки определения на оригинал, заверено копие или заверен превод. Неговата цел се ограничава до улесняване на проверката на електронните подписи, използвани в оригиналните документи, заверените копия или заверените преводи, които доставчиците на услуги евентуално трябва да представят посредством единичните звена за контакт.

[1] ОВ L 376, 27.12.2006 г., стр. 36.
[2] ОВ L 274, 20.10.2009 г., стр. 36.

(6) За да се даде възможност на държавите-членки да внедрят необходимите технически средства, е уместно настоящото решение да се прилага от 1 август 2011 г.

(7) Мерките, предвидени в настоящото решение, са в съответствие със становището на Комитета по Директивата за услугите,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Референтен формат за електронните подписи

1. Държавите-членки въвеждат необходимите технически средства, позволяващи им да обработват електронно подписаните документи, които са предоставени посредством единичните звена за контакт от доставчиците на услуги с оглед приключването на съответните процедури и формалности съгласно член 8 от Директива 2006/123/ЕО и които са подписани от компетентните органи на други държави-членки с усъвършенствани електронни подписи от типа XML, CMS или PDF във формат BES или EPES, съответстващ на изложените в приложението технически спецификации.

2. Държавите-членки, чиито компетентни органи използват за подписването на посочените в параграф 1 документи формати на електронни подписи, различни от посочените във въпросния параграф, уведомяват Комисията за съществуващите възможности за валидиране, чрез които другите държави-членки могат да валидират получените електронни подписи онлайн, безплатно и по начин, който е разбираем за лицата, които не са носители на езика, освен когато необходимата информация вече е била включена в документа, в електронния подпис или в носителя на електронния документ. Комисията ще предостави тази информация на всички държави-членки.

Член 2

Прилагане

Настоящото решение се прилага от 1 август 2011 г.

Член 3

Адресати

Адресати на настоящото решение са държавите-членки.

Съставено в Брюксел на 25 февруари 2011 година.

За Комисията

Michel BARNIER

Член на Комисията

ПРИЛОЖЕНИЕ

Спецификации на усъвършенствани електронни подписи (XML, CMS или PDF), които трябва да бъдат технически поддържани от получаващата държава-членка

В следващата част от документа ключовите думи „ТРЯБВА“, „НЕ ТРЯБВА/ТРЯБВА ДА НЕ“, „ЗАДЪЛЖИТЕЛЕН“, „СЛЕДВА“, „НЕ СЛЕДВА“, „БИ ТРЯБВАЛО“, „НЕ БИ ТРЯБВАЛО“, „ПРЕПОРЪЧИТЕЛЕН“, „МОЖЕ“ и „НЕЗАДЪЛЖИТЕЛЕН“ следва да се интерпретират в съответствие с термините на английски, описани в RFC 2119 ([1]).

РАЗДЕЛ 1 — XAdES-BES/EPES

Подписът съответства на спецификациите за подпис от типа W3C XML ([2])

Подписът ТРЯБВА да бъде поне във формат XAdES-BES (или -EPES) съгласно спецификациите ETSI TS 101 903 XAdES ([3]) и да съответства на всички долупосочени допълнителни спецификации:

С ds:CanonicalizationMethod, уточняващ алгоритъма за канонизация (canonicalization algorithm), прилаган спрямо елемента SignedInfo преди извършването на изчисленията на подписа, се определя единствено някой от следните алгоритми:

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

Други алгоритми или версии „с коментари“ на горепосочените алгоритми НЕ СЛЕДВА да се използват за създаването на подписи, но СЛЕДВА да бъдат поддържани с оглед остатъчната оперативна съвместимост за проверката на подписи.

MD5 (RFC 1321) НЕ ТРЯБВА да бъде използван като дайджест алгоритъм (digest algorithm). Подписващите биват насочени към приложимото национално законодателство, а по отношение на насоките — към ETSI TS 102 176 ([4]), както и към ECRYPT2 D.SPA.x report ([5]) за допълнителни препоръки във връзка с алгоритмите и параметрите, приложими за електронните подписи.

Използването на *трансформации* е ограничено до посочените по-долу:

Canonicalization transforms: вж. съответните спецификации по-горе;

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

Filtering:

XPath (http://www.w3.org/TR/1999/REC-xpath-19991116): с оглед на съвместимостта и съпоставимостта с XMLDSig

XPath Filter 2.0 (http://www.w3.org/2002/06/xmldsig-filter2): като наследник на XPath вследствие на експлоатационни проблеми

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

XSLT (набор от стилове) **transform**.

Елементът ds:KeyInfo ТРЯБВА да включва дигиталното удостоверение на подписващия X.509 v3 (т.е. посочва се и неговата стойност).

Подписаните характеристики на подписа SigningCertificate ТРЯБВА да включват дайджест стойността (CertDigest) и IssuerSerial на удостоверението на подписващия, съхранявано в ds:KeyInfo, а незадължителното URI в SigningCertificate НЕ ТРЯБВА да бъде използвано.

Подписаните характеристики на подписа SigningTime се показват и съдържат UTC под формата на xsd:dateTime (http://www.w3.org/TR/xmlschema-2/#dateTime).

Елементът DataObjectFormat ТРЯБВА да бъде представен и да съдържа поделемент MimeType.

Когато използваните от държавите-членки подписи са базирани на квалифицирано удостоверение, включените в подписите PKI обекти (вериги от удостоверения, анулирани данни, времеви маркери) се проверяват съгласно Решение 2009/767/ЕО чрез доверителния списък на държавите-членки, които контролират или акредитират одобрения доставчик на услуги.

В таблица 1 са обобщени спецификациите, които подписът във формат XAdES-BES/EPES трябва да покрие, за да бъде технически поддържан от получаващата държава-членка.

([1]) IETF RFC 2119: „Ключови думи, използвани в документация от тип RFC за обозначаване на различните нива на изискванията“.
([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 v.1.4.1: 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]) Последна версия D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010) от 30 март 2010 г. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Таблица 1

XAdES - BES (EPES)		**Общи минимални изисквания**
(ETSI TS 103 903 се прилага заедно със следните профилирани елементи)		
З = задължително; Н = незадължително; П = препоръчително; Не = не се прилага		
ds: Signature ID	З	
ds: SignedInfo	З	
ds: CanonicalizationMethod	З	*Всеки един от долупосочените алгоритми ТРЯБВА да бъде поддържан за проверка на подписа; създаването СЛЕДВА да се ограничава върху един от следните:* *- 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* *Други методи или "#WithComments" версии на горепосочените НЕ СЛЕДВА да се използват.*
ds: SignatureMethod	З	***Алгоритми:*** *препратки към приложимото национално законодателство, към ETSI TS 102 176 за насоки и към доклада ECRYPT2 D.SPA.7 за допълнителни препоръки.*
ds: Reference URI	З	Една препратка към всеки първоначален обект от данни, подлежащ на подписване (URI могат да насочват и към външни обекти), + препратка към елемент SignedProperties
ds: Transforms	Н	*Приложенията за проверка ТРЯБВА да поддържат всяка една от следните платформи; докато приложението за създаване на подпис СЛЕДВА да ограничи използването на тези платформи до следните:* *- Canonicalization transforms: вж. по-горе* *- Base64 encoding* *- XPath и XPath Filter 2.0* *- Enveloped signature transform* *- XSLT transforms*
ds: DigestMethod	З	***Алгоритми:*** *препратки към приложимото национално законодателство, към ETSI TS 102 176 за насоки и към доклада ECRYPT2 D.SPA.7 за допълнителни препоръки.*
ds: DigestValue	З	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	З	
ds: KeyInfo	З	ТРЯБВА да съдържа удостоверение X509 (подписаните характеристики на SigningCertificate ТРЯБВА да съдържат дайджест стойността на удостоверението на подписващия) Веригите от удостоверения на подписващия е ПРЕПОРЪЧИТЕЛНО да бъдат посочени с оглед улесняване на процеса на валидиране (в тези случаи ТРЯБВА да се представят удостоверения)
ds: Object		
QualifyingProperties	З	
SignedProperties	З	З
SignedSignatureProperties	З	З
SigningTime	З	UTC (xsd: dateTime).
SigningCertificate	З	ТРЯБВА да съдържа дайджест стойността на удостоверението на подписващия, съхранявано в ds:KeyInfo и факултативното URI се пропуска (приложенията МОГАТ да търсят/намерят удостоверението на подписващия в ds:KeyInfo въз основа на хеш еквивалент).
SignaturePolicyIdentifier	Н	само във формат EPES (и за по-висши формати, базирани на EPES)
Signature ProductionPlace	Н	
SignerRole	Н	
/SignedSignatureProperties		
SignedDataObjectProperties	Н	
DataObjectFormat	З	При използването на това поле приложенията СЛЕДВА да гарантират, че обектите от данни са съответно показани на потребителя. При ползване ТРЯБВА да се използва поделемент MimeType.
CommitmentTypeIndication	Н	
AllDataObjectsTimeStamp	Н	
IndividualDataObjectTimeStamp	Н	
/SignedDataObjectProperties		
/SignedProperties		
UnsignedProperties	Н	
UnsignedSignatureProperties		
CounterSignature	Н	
/UnsignedSignatureProperties		
/UnsignedProperties		
/QualifyingProperties		
/ds: Object		
/ds: Signature		
Топология на подписите — Пакетно подписани първоначални данни и подписи		
SignatureEnveloped		Всички ТРЯБВА да бъдат поддържани
SignatureEnveloping		
SignatureDetached		

РАЗДЕЛ 2 — CADES-BES/EPES

Подписът съответства на спецификациите за подпис от типа Cryptographic Message Syntax (CMS) [1].

Подписът използва атрибутите CAdES-BES (или -EPES) съгласно спецификациите ETSI TS 101 733 CAdES [2] и съответства на допълнителните спецификации, посочени в таблица 2 по-долу.

Всички атрибути на CAdES, включени в хеш изчислението на архивираните времеви маркери (ETSI TS 101 733 v.1.8.1 Annex K), ТРЯБВА да бъдат кодирани съгласно DER, а всички други — съгласно BER, за да се опрости еднократната обработка на CAdES.

MD5 (RFC 1321) НЕ ТРЯБВА да бъде използван като дайджест алгоритъм (digest algorithm). Подписващите биват насочени към приложимото национално законодателство, а по отношение на насоките — към ETSI TS 102 176 [3], както и към ECRYPT2 D.SPA.x report [4] за допълнителни препоръки във връзка с алгоритмите и параметрите, приложими за електронните подписи.

Подписаните атрибути ТРЯБВА да включват препратка към дигиталното удостоверение на подписващия X.509 v3 (RFC 5035) и в полето *SignedData.certificates* ТРЯБВА да се посочи неговата стойност.

Подписаният атрибут SigningTime ТРЯБВА да бъде посочен и ТРЯБВА да съдържа UTC, представено както в http://tools.ietf.org/html/rfc5652#section-11.3.

Подписаният атрибут ContentType ТРЯБВА да бъде посочен и да съдържа идентификационни данни (http://tools.ietf.org/html/rfc5652#section-4), като се предвижда типът на съдържанието на данните да съответства на произволна октетна последователност (arbitrary octet strings), като например UTF-8 text или ZIP носител с поделемент MimeType.

Когато използваните от държавите-членки подписи са базирани на квалифицирано удостоверение, включените в подписите PKI обекти (вериги от удостоверения, анулирани данни, времеви маркери) се проверяват съгласно Решение 2009/767/ЕО чрез доверителния списък на държавата-членка, която контролира или акредитира одобрения доставчик на услуги.

---

[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] Последна версия D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010) от 30 март 2010 г. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Таблица 2

CAdES - BES (EPES)		**Общи минимални изисквания**
(ETSI TS 101 733 се прилага заедно със следните профилирани елементи)		
ASN.1		
`ContentInfo ::= SEQUENCE {`		
`contentType ContentType, -- id-signedData`		
`content [0] EXPLICIT ANY DEFINED BY contentType }`		
З = задължително; Н = незадължително; П = препоръчително; Не = не се прилага		
`SignedData ::= SEQUENCE {`		
`version CMSVersion,`		
`digestAlgorithms DigestAlgorithmIdentifiers,`	З	**Алгоритми**: препратки към приложимото национално законодателство, към ETSI TS 102 176 за насоки и към доклада ECRYPT2 D.SPA.7 за допълнителни препоръки.
`encapContentInfo SEQUENCE {`		
`eContentType ContentType,`	З	id-Data
`eContent [0] EXPLICIT OCTET STRING OPTIONAL -- not present if signature is detached },`	З/Не	Подписаният атрибут ContentType е наличен и съдържа идентификационни данни (http://tools.ietf.org/html/rfc5652#section-4), като се предвижда типът на съдържанието на данните да съответства на произволна октетна последователност, като UTF-8 text или ZIP носител с поделемент MimeType
`-- External Data (if signature detached)*`		Налично само при отделен подпис. * Външни данни представляват данни, защитени чрез отделен подпис, който не е включен като eContent на подпис с формат CAdES. Препоръчва се подписаните външни данни да се обединят с подписа в ZIP файл.
`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	З	ТРЯБВА да съдържа удостоверение X509 от подписващия. Включването на удостоверения от цялата верига на удостоверения до крайната точка на доверие (trust anchor) е ПРЕПОРЪЧИТЕЛНО.
`crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,`	Н	
`signerInfos SET OF`	З	Поне едно signerInfo
`SEQUENCE { -- SignerInfo`		
`version CMSVersion,`		
`sid SignerIdentifier,`	Ф	(Незащитена стойност)
`digestAlgorithm DigestAlgorithmIdentifier,`	З	**Алгоритми**: препратки към приложимото национално законодателство, към ETSI TS 102 176 за насоки и към доклада ECRYPT2 D.SPA.7 за допълнителни препоръки.
`signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF`		
`SEQUENCE { -- Attribute`	З	
`attrType OBJECT IDENTIFIER,`	З/Не	**ТРЯБВА**: id-contentType (с идентификационни данни) id-messageDigest id-aa-ets-signingCertificateV2 или id-aa-signingCertificate ТРЯБВА: signingTime **НЕЗАДЪЛЖИТЕЛНО**: id-aa-ets-sigPolicyId Други незадължителни атрибути, определени в ETSI TS 101 733.
`attrValues SET OF AttributeValue } OPTIONAL,`		
`signatureAlgorithm SignatureAlgorithmIdentifier,`		**Алгоритми**: препратки към приложимото национално законодателство, към ETSI TS 102 176 за насоки и към доклада ECRYPT2 D.SPA.7 за допълнителни препоръки.
`signature OCTET STRING, -- SignatureValue`		
`unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF`	Н	
`SEQUENCE { attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }`	Н	

РАЗДЕЛ 3 — PADES-PART 3 (BES/EPES)

Подписът ТРЯБВА да използва разширенията PAdES-BES (или -EPES) съгласно спецификациите ETSI TS 102 778 PAdES-Part3 ([1]) и да съответства на долупосочените допълнителни спецификации:

MD5 (RFC 1321) НЕ ТРЯБВА да бъде използван като дайджест алгоритъм (digest algorithm). Подписващите биват насочени към приложимото национално законодателство, а по отношение на насоките — към ETSI TS 102 176 ([2]), както и към ECRYPT2 D.SPA.x report ([3]) за допълнителни препоръки във връзка с алгоритмите и параметрите, приложими за електронните подписи.

Подписаните атрибути ТРЯБВА да включват препратка към дигиталното удостоверение на подписващия X.509 v3 (RFC 5035) и в полето *SignedData.certificates* ТРЯБВА да се посочи неговата стойност;

([1]) ETSI TS 102 778-3 v.1.2.1: 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]) Последна версия D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009–2010) от 30 март 2010 г. (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

Времето на подписване се посочва чрез стойността на запис M в речника на подписа.

Когато използваните от държавите-членки подписи са базирани на квалифицирано удостоверение, включените в подписите PKI обекти (вериги от удостоверения, анулирани данни, времеви маркери) се проверяват съгласно Решение 2009/767/ЕО чрез доверителния списък на държавата-членка, която контролира или акредитира одобрения доставчик на услуги.