РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2017/2288 НА КОМИСИЯТА

от 11 декември 2017 година

за определяне на технически спецификации в областта на информационните и комуникационните технологии, които да служат за посочване като еталон при обществените поръчки

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета ([1]), и по-специално член 13, параграф 1 от него,

след консултация с Европейската многостранна платформа по въпросите на стандартизацията в областта на информационните и комуникационните технологии (ИКТ) и с експерти от сектора,

като има предвид, че:

(1) Стандартизацията играе важна роля за изпълнението на стратегията „Европа 2020“ ([2]). В няколко водещи инициативи на стратегията „Европа 2020“ се подчертава значението на доброволната стандартизация на пазарите на стоки или услуги, за да се гарантират съгласуваността и оперативната съвместимост между стоките и услугите, да се насърчи технологичното развитие и да се подпомогнат нововъведенията.

(2) Стандартите са от съществено значение за европейската конкурентоспособност, както и за нововъведенията и напредъка. В съобщенията на Комисията за единния пазар ([3]) и за цифровия единен пазар ([4]) се потвърждава значението на общите стандарти за осигуряване на необходимата оперативна съвместимост на мрежите и системите на европейската цифрова икономика. Това становище се подсилва допълнително с приемането на Съобщението „Приоритети за стандартизацията в областта на ИКТ за цифровия единен пазар“ ([5]), където Комисията определя приоритетните ИКТ, при които се смята, че стандартизацията има решаващо значение за завършването на цифровия единен пазар.

(3) В Съобщението на Комисията „Стратегическа визия за европейските стандарти: към по-голям и ускорен устойчив растеж на европейската икономика до 2020 г.“ ([6]) се признава специфичният характер на стандартизацията в областта на ИКТ, в която различните решения, приложения и услуги често се разработват от световни форуми и обединения за ИКТ, явяващи се водещи организации за разработване на стандарти за ИКТ.

(4) С Регламент (ЕС) № 1025/2012 относно европейската стандартизация се създава система, посредством която Комисията може да реши да определи онези технически спецификации в областта на ИКТ, които са най-значими и най-широко възприети и са издадени от организации, различни от европейски, международни или национални организации по стандартизация, и които може да бъдат посочвани като еталон главно с цел осигуряване на оперативна съвместимост при обществените поръчки. Възможността за използване на пълния набор от технически спецификации в областта на ИКТ при обществените поръчки за апаратно и програмно осигуряване и услуги в сферата на информационните технологии ще позволи постигането на оперативна съвместимост между устройствата, услугите и приложенията, ще помогне на държавните администрации да предотвратят зависимостта от доставчика, когато възложителите на обществени поръчки не могат да го сменят след изтичането на договора за възлагане на обществена поръчка поради използването на ИКТ решения със затворен код и ще насърчи конкуренцията при предлагането на оперативно съвместими ИКТ решения.

(5) За да бъдат допустими за посочване като еталон при обществените поръчки, техническите спецификации в областта на ИКТ трябва да отговарят на изискванията, посочени в приложение II към Регламент (ЕС) № 1025/2012. Спазването на тези изисквания осигурява увереност на публичните органи, че техническите спецификации в областта на ИКТ са установени в съответствие с принципите на прозрачност, откритост, безпристрастност и консенсус, признати от Световната търговска организация (СТО) в областта на стандартизацията.

([1]) ОВ L 316, 14.11.2012 г., стр. 12.
([2]) Съобщение на Комисията „Европа 2020 – Стратегия за интелигентен, устойчив и приобщаващ растеж“. COM(2010) 2020 окончателен, 3 март 2010 г.
([3]) Съобщение на Комисията „Осъвременяване на единния пазар: повече възможности за гражданите и предприятията.“ COM(2015) 550 final, 28 октомври 2015 г.
([4]) Съобщение „Стратегия за цифров единен пазар за Европа“. COM(2015) 192 final, 6 май 2015 г.
([5]) COM (2016)176 final, 19 април 2016 г.
([6]) COM(2011) 311 окончателен, 1 юни 2011 г.

(6) Решението за определяне на спецификацията в областта на ИКТ трябва да бъде взето след консултация с Европейската многостранна платформа по въпросите на стандартизацията в областта на ИКТ, създадена с Решение 2011/C 349/04 на Комисията ([1]), допълнена от други форми на консултация с експерти от сектора.

(7) Европейската многостранна платформа по въпросите на стандартизацията в областта на ИКТ извърши оценка и даде положително становище за определянето на следните технически спецификации за посочване като еталон при обществените поръчки: „SPF-Sender Policy Framework for Authorizing Use of Domains in Email“ („SPF“), „STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security“ („STARTTLS-SMTP“) и „DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security“ („DANE- SMTP“), разработени от Работната група за интернет инженеринг (Internet Engineering Task Force – IETF); „Structured Threat Information Expression“ („STIX 1.2“) и „Trusted Automated Exchange of Indicator Information“ („TAXII 1.1“), разработени от Организацията за усъвършенстване на структурираните информационни стандарти (Organization for the Advancement of Structured Information Standards – OASIS). Впоследствие оценката и становището на Платформата бяха представени за консултация с експерти от сектора, които потвърдиха положителното становище относно определянето на тези спецификации.

(8) Техническата спецификация „SPF“, разработена от IETF, е отворен стандарт, с който се определя техническият метод за установяване дали е подправен адресът на изпращача. „SPF“ осигурява възможност за проверка дали дадено съобщение е изпратено от сървър, който има необходимото за тази цел разрешение. Това е проста система за потвърждаване за електронната поща, която е предназначена да установява дали е подправен адресът на изпращача, като осигурява механизъм, позволяващ разпределителите на поща да проверяват дали входящата поща от даден домейн идва от хост с разрешение от администраторите на този домейн. Предназначението на „SPF“ е да се попречи на разпространителите на нежелани съобщения да изпращат такива съобщения с подправен адрес на изпращача в даден домейн. Получателите могат да направят справка в запис на „SPF“, за да определят дали дадено съобщение, обозначено като идващо от този домейн, идва от сървър за електронна поща с необходимото разрешение.

(9) „STARTTLS-SMTP“, разработен от IETF, е способ за подобряване на дадена незащитена връзка до защитена връзка. STARTTLS е разширение на опростения протокол за обмен на електронна поща („Simple Mail Transfer Protocol – SMTP“), чрез който даден SMTP сървър и клиент може да използва Transport Layer Security (TLS), за да предава лични съобщения с удостоверяване на самоличността в интернет. Незащитените съобщения по електронната поща са особено значим канал за атакуване на държавните съобщителни мрежи и незаконно проникване в тях. Ако даден потребител изпраща електронно писмо, пощенският сървър на доставчика на пощенски услуги на потребителя ще изпрати това писмо до пощенския сървър на получателя. Връзката между тези два пощенски сървъра може да бъде защитена предварително чрез TLS. Чрез STARTTLS се осигурява способ за подобряване на некриптирана (с формат „plain-text“) връзка до криптирана TLS връзка.

(10) „DANE-SMTP“, разработени от IETF, са поредица от протоколи за повишаване на сигурността в интернет, които дават възможност за поставяне на ключове в системата от имена на домейните (Domain Name System – DNS) и за защитаването им чрез DNSSEC (DNS Security, протокол за разширения за сигурност на системата от имена на домейните). Когато се установява защитена връзка с неизвестно лице, желателно е в режим „на линия“ да се извърши проверка на самоличността на изпращача и местоназначението. Това може да се извърши чрез сертификати, издадени от сертифициращи организации в рамките на системата за инфраструктурата на публичния ключ (PKI), или чрез саморъчно подписани сертификати. Чрез DANE се осигурява възможност на притежателя на домейн (наричан „регистрант“) да предостави още информация като допълнение към сертификатите в режим „на линия“ чрез DNS запис, защитен чрез DNSSEC. Следователно DANE са особено важни за борбата с активните нападатели на съобщителните мрежи.

(11) „STIX 1.2“, разработен от OASIS, е език за стандартизирано и структурирано описание на информацията за кибернетичните заплахи. Той обхваща важни теми, свързани с данните за кибернетични заплахи, като улеснява анализирането и обмена на информация за атаките. Той характеризира обширен набор от данни за кибернетичните заплахи, в т.ч. признаци за враждебна дейност, например IP адреси и кодове за сегментиране на файлове (file hashes), както и контекстуална информация за заплахите, например враждебна тактика, техника и процедури (Tactics, Techniques and Procedures – TTPs); експлоатационни цели; кампании и поредици от действия (Campaigns and Courses of Action – COA). Тази информация в своята съвкупност напълно характеризира мотивите, способностите и действията на кибернетичния враг и по този начин спомага за защитата при атаки.

(12) „TAXII v1.1“ е техническа спецификация, също разработена от OASIS, с която се стандартизира надеждният автоматизиран обмен на информация за кибернетичните заплахи. С TAXII се определят услугите и обменът на съобщения за споделяне на практическа информация за кибернетичните заплахи в цялата организация, за всички продукти или за всички услуги с оглед на установяването, предотвратяването и ограничаването на кибернетичните заплахи. С TAXII на организациите се осигурява възможност да повишават осведомеността в конкретни случаи на възникващи заплахи и лесно да споделят информация с партньорите си, използвайки съществуващите отношения и системи,

([1]) Решение 2011/C 349/04 на Комисията от 28 ноември 2011 г. за създаване на Европейска многостранна платформа по въпросите на стандартизацията в областта на ИКТ (ОВ C 349, 30.11.2011 г., стр. 4).

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Посочените в приложението технически спецификации са допустими за посочване като еталон при обществените поръчки.

Член 2

Настоящото решение влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 11 декември 2017 година.

За Комисията
Председател
Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ

Работна група за интернет инженеринг (Internet Engineering Task Force – IETF)

№	Заглавие на техническата спецификация в областта на ИКТ
1	SPF-Sender Policy Framework
2	STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security
3	DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (TLS)

Организация за усъвършенстване на структурираните информационни стандарти (Organization for the Advancement of Structured Information Standards – OASIS)

№	Заглавие на техническата спецификация в областта на ИКТ
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information