DECIZIA DE PUNERE ÎN APLICARE (UE) 2017/2288 A COMISIEI

din 11 decembrie 2017

privind identificarea specificațiilor tehnice TIC destinate utilizării drept referințe în procedurile de achiziții publice

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului ([1]), în special articolul 13 alineatul (1),

după consultarea Forumului european multipartit privind standardizarea în domeniul TIC, precum și a experților din sector,

întrucât:

(1) Standardizarea joacă un rol important în susținerea strategiei Europa 2020 ([2]). Mai multe inițiative emblematice ale strategiei Europa 2020 au subliniat importanța standardizării voluntare de pe piețele de produse sau servicii pentru a asigura compatibilitatea și interoperabilitatea între produse și servicii, a promova dezvoltarea tehnologică și a sprijini inovarea.

(2) Standardele sunt esențiale pentru competitivitatea europeană și indispensabile pentru inovare și progres. Comunicările Comisiei privind piața unică ([3]) și piața unică digitală ([4]) confirmă relevanța standardelor comune pentru a asigura interoperabilitatea necesară a rețelelor și sistemelor în economia digitală europeană. Acest lucru este consolidat prin adoptarea Comunicării privind prioritățile de standardizare în sectorul TIC ([5]), în cadrul căreia Comisia identifică tehnologiile TIC prioritare în care standardizarea este considerată esențială pentru finalizarea pieței unice digitale.

(3) Comunicarea Comisiei intitulată „O viziune strategică pentru standardele europene: avansând în direcția îmbunătățirii și accelerării creșterii durabile a economiei europene până în 2020” ([6]) a recunoscut specificitatea standardizării în domeniul tehnologiilor informației și comunicațiilor (TIC), în care soluțiile, aplicațiile și serviciile sunt deseori elaborate de forumuri și consorții TIC mondiale care conduc în prezent organizațiile implicate în elaborarea de standarde TIC.

(4) Regulamentul (UE) nr. 1025/2012 privind standardizarea europeană a stabilit un sistem prin care Comisia poate decide să identifice cele mai relevante și mai larg acceptate specificații tehnice TIC elaborate de organizații care nu sunt organizații de standardizare europene, internaționale sau naționale, care pot fi ulterior standardizate, în principal pentru a permite interoperabilitatea în cadrul achizițiilor publice. Posibilitatea de a utiliza întreaga gamă de specificații tehnice TIC în momentul achiziționării de hardware, de software și de servicii de tehnologia informației va facilita interoperabilitatea dintre dispozitive, servicii și aplicații, va contribui la evitarea blocajelor în administrațiile publice care se produc atunci când autoritatea contractantă nu poate să schimbe un furnizor după expirarea contractului de achiziție publică deoarece utilizează soluții TIC proprietare și va încuraja concurența în domeniul furnizării de soluții TIC interoperabile.

(5) Pentru ca specificațiile tehnice TIC să poată fi utilizate drept referințe în procedurile de achiziții publice, ele trebuie să respecte cerințele prevăzute în anexa II la Regulamentul (UE) nr. 1025/2012. Conformitatea cu cerințele respective garantează autorităților publice că specificațiile tehnice TIC sunt stabilite în conformitate cu principiile deschiderii, transparenței, imparțialității și consensului recunoscute de Organizația Mondială a Comerțului în domeniul standardizării.

([1]) JO L 316, 14.11.2012, p. 12.
([2]) Comunicarea Comisiei intitulată „Europa 2020: O strategie europeană pentru o creștere inteligentă, durabilă și favorabilă incluziunii”. COM(2010) 2020 final, 3 martie 2010.
([3]) Comunicarea Comisiei „Ameliorarea pieței unice: mai multe oportunități pentru cetățeni și pentru întreprinderi”. COM(2015) 550 final din 28 octombrie 2015.
([4]) Comunicarea „O strategie privind piața unică digitală pentru Europa”. COM(2015) 192 final din 6 mai 2015.
([5]) COM(2016) 176 final din 19 aprilie 2016.
([6]) COM (2011) 311 final din 1 iunie 2011.

(6) Decizia de a identifica specificațiile TIC trebuie să fie adoptată după consultarea Forumului european multipartit privind standardizarea în domeniul TIC instituit prin Decizia 2011/C 349/04 a Comisiei ([1]), completată cu alte forme de consultare a experților din sector.

(7) Forumul european multipartit privind standardizarea în domeniul TIC a evaluat identificarea următoarelor specificații tehnice destinate utilizării drept referințe în procedurile de achiziții publice și a emis un aviz favorabil în acest sens: „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»)" și „DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security («DANE- SMTP»)" dezvoltate de Internet Engineering Task Force (IETF); „Structured Threat Information Expression («STIX 1.2»)" și „Trusted Automated Exchange of Indicator Information («TAXII 1.1»)" dezvoltate de OASIS (*Organization for the Advancement of Structured Information Standards* – Organizația pentru promovarea standardelor privind informațiile structurate). Evaluarea și avizul forumului au fost transmise ulterior spre consultare experților sectoriali, care au confirmat avizul favorabil în ceea ce privește identificarea.

(8) Specificația tehnică „SPF" dezvoltată de IETF este un standard deschis care specifică o metodă tehnică pentru detectarea falsificării adresei expeditorului. SPF oferă posibilitatea de a verifica dacă un mesaj este transmis de pe un server autorizat în acest sens. Este un sistem de validare a e-mailurilor destinat să detecteze falsificarea adreselor de e-mail (*spoofing*) cu ajutorul unui mecanism care permite destinatarului unui e-mail să verifice dacă e-mailul transmis de un domeniu provine de la un expeditor autorizat de administratorii domeniului respectiv. Scopul SPF este de a împiedica expeditorii de spamuri să trimită mesaje de la adrese de origine falsificate către un anumit domeniu. Destinatarii pot face apel la o înregistrare SPF pentru a stabili dacă un mesaj care pretinde că provine de la domeniul respectiv este transmis de un server de e-mail autorizat.

(9) Specificația „STARTTLS-SMTP" dezvoltată de IETF reprezintă o modalitate de a transforma o conexiune nesecurizată într-o conexiune securizată. STARTTLS reprezintă o extindere a serviciului SMTP (*Simple Mail Transfer Protocol*) care permite unui server și client SMTP să utilizeze protocolul TLS (*Transport Layer Security*) pentru a oferi o comunicare privată și autentificată pe internet. Comunicarea prin e-mail nesecurizat reprezintă un important vector de atac la adresa rețelelor autorităților publice. Atunci când utilizatorul trimite un e-mail, serverul de e-mail al utilizatorului va trimite acest e-mail serverului de e-mail al destinatarului. Conexiunea dintre aceste servere de e-mail poate fi securizată în avans cu TLS. STARTTLS oferă o modalitate de a transforma o conexiune necriptată (text simplu) într-o conexiune criptată TLS.

(10) Specificația „DANE-SMTP" dezvoltată de IETF este un set de protocoale pentru sporirea securității internetului care permite introducerea unor chei în sistemul de nume de domenii (DNS) și securizarea acestuia prin protocolul DNSSEC („DNS Security"). Atunci când se stabilește o conexiune securizată cu o entitate necunoscută, este de dorit să se verifice online autenticitatea expeditorului și a destinației. Acest lucru poate fi realizat prin certificate eliberate de autoritățile de certificare („AC") în cadrul sistemului PKI sau prin certificate autosemnate. DANE permite deținătorului unui domeniu („solicitantul înregistrării") să furnizeze informații suplimentare, pe lângă certificatele online, prin intermediul unei înregistrări DNS securizate prin DNSSEC. DANE este, prin urmare, deosebit de importantă pentru combaterea atacatorilor activi.

(11) Specificația „STIX 1.2", dezvoltată de OASIS, este un limbaj pentru descrierea informațiilor privind amenințările cibernetice într-un mod standardizat și structurat. Specificația acoperă teme importante în materie de date legate de amenințările cibernetice, facilitând analiza și schimbul de informații cu privire la atacuri. Ea definește un set cuprinzător de informații privind amenințările cibernetice, inclusiv indicatori ai activităților rău-intenționate cum ar fi adresele IP și valorile hash ale fișierelor și informații contextuale privind amenințări precum tactici, tehnici și proceduri rău-intenționate („TTP"); obiective de exploatare; campanii și modalități de acțiune („COA"). Toate aceste informații permit definirea completă a motivațiilor, capacităților și activităților atacatorilor cibernetici și, prin urmare, contribuie la apărarea împotriva atacurilor.

(12) Specificația tehnică „TAXII v1.1" dezvoltată de OASIS standardizează schimbul automat și securizat de informații privind amenințările cibernetice. TAXII definește serviciile și schimburile de mesaje pentru partajarea de informații privind amenințările cibernetice între organizații, produse sau servicii în vederea detectării, prevenirii și reducerii amenințărilor cibernetice. Prin intermediul specificației TAXII, organizațiile pot să cunoască mai bine amenințările emergente, pot să facă mai ușor schimb de informații cu partenerii, folosind în același timp relațiile și sistemele existente,

([1]) Decizia 2011/C 349/04 a Comisiei din 28 noiembrie 2011 de înființare a Forumului european multipartit privind standardizarea în domeniul TIC (JO C 349, 30.11.2011, p. 4).

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Specificațiile tehnice enumerate în anexă sunt eligibile pentru utilizarea ca referințe în cadrul achizițiilor publice.

Articolul 2

Prezenta decizie intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 11 decembrie 2017.

Pentru Comisie
Președintele
Jean-Claude JUNCKER

ANEXĂ

Internet Engineering Task Force (IETF)

Nr.	Titlul specificației tehnice TIC
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)

Organization for the Advancement of Structured Information Standards (OASIS)

Nr.	Titlul specificației tehnice TIC
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information