KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2017/2288

(2017. gada 11. decembris)

par to IKT tehnisko specifikāciju noteikšanu, uz kurām var atsaukties publiskajā iepirkumā

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2012. gada 25. oktobra Regulu (ES) Nr. 1025/2012 par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK ([1]), un jo īpaši tās 13. panta 1. punktu,

apspriedusies Eiropas daudzpusējā ieinteresēto personu forumā IKT standartizācijas jautājumos un ar nozares ekspertiem,

tā kā:

(1) Standartizācijai ir svarīga nozīme stratēģijas "Eiropa 2020" ([2]) atbalstīšanā. Vairākās stratēģijas "Eiropa 2020" pamatiniciatīvās uzsvērts, ka preču un pakalpojumu saderības un sadarbspējas nodrošināšanā, tehnikas attīstības veicināšanā un inovācijas sekmēšanā liela nozīme ir brīvprātīgai standartizācijai preču vai pakalpojumu tirgos.

(2) Standarti ir būtiski Eiropas konkurētspējai, un no tiem ir atkarīga inovācija un progress. Tas, ka kopēji standarti ir svarīgi, lai nodrošinātu tīklu un sistēmu savstarpējo sadarbspēju Eiropas digitālajā ekonomikā, apstiprināts Komisijas paziņojumā par vienoto tirgu ([3]) un paziņojumā par digitālo vienoto tirgu ([4]). Tas ir nostiprināts, Komisijai pieņemot paziņojumu par IKT standartizācijas prioritātēm ([5]), kurā tā nosaka prioritārās IKT tehnoloģijas, kuras ir būtiskas digitālā vienotā tirgus izveides pabeigšanai.

(3) Komisijas paziņojumā "Eiropas standartu stratēģisks redzējums: virzības mērķis – līdz 2020. gadam sekmēt un paātrināt ilgtspējīgu Eiropas ekonomikas izaugsmi" ([6]) atzīts, ka informācijas un komunikācijas tehnoloģiju (IKT) standartizācijas process ir visai specifisks, proti, IKT risinājumus, lietojumus un pakalpojumus bieži izstrādā pasaules mēroga IKT forumi un konsorciji, un tie arī izvirzījušies par vadošajām IKT standartu izstrādes organizācijām.

(4) Ar Regulu (ES) Nr. 1025/2012 par Eiropas standartizāciju ir izveidota sistēma, kas ļauj Komisijai pieņemt lēmumu noteikt nozīmīgākās un izplatītākās IKT tehniskās specifikācijas, kuras izdevušas organizācijas, kas nav Eiropas, starptautiskās vai valstu standartizācijas organizācijas, un uz kurām varētu atsaukties, galvenokārt lai nodrošinātu sadarbspēju publiskajā iepirkumā. Iespēja izmantot visu IKT tehnisko specifikāciju klāstu, iepērkot aparatūru, programmatūru un informācijas tehnoloģiju pakalpojumus, padarīs iespējamu sadarbspēju starp ierīcēm, pakalpojumiem un lietotnēm, palīdzēs pārvaldes iestādēm nenonākt strupceļā, kad publiskā iepirkuma rīkotājs pēc iepirkuma līguma termiņa beigām nevar nomainīt pakalpojuma sniedzēju tāpēc, ka izmanto tam piederošus IKT risinājumus, un veicinās konkurenci sadarbspējīgu IKT risinājumu piegādē.

(5) Lai uz IKT tehniskajām specifikācijām drīkstētu atsaukties publiskajā iepirkumā, tām ir jāatbilst Regulas (ES) Nr. 1025/2012 II pielikumā izklāstītajām prasībām. Minēto prasību ievērošana publiskajām iestādēm garantē, ka IKT tehniskās specifikācijas ir noteiktas saskaņā ar atklātuma, pārredzamības, objektivitātes un konsensa principiem, ko standartizācijas jomā atzīst Pasaules Tirdzniecības organizācija.

([1]) OV L 316, 14.11.2012., 12. lpp.
([2]) Komisijas Paziņojums "Eiropa 2020 – stratēģija gudrai, ilgtspējīgai un integrējošai izaugsmei". COM(2010) 2020 galīgā redakcija, 2010. gada 3. marts.
([3]) Komisijas paziņojums "Vienotā tirgus pilnīgošana – plašākas iespējas cilvēkiem un uzņēmējdarbībai", COM(2015) 550 final, 2015. gada 28. oktobris.
([4]) Paziņojums par Digitālā vienotā tirgus stratēģiju Eiropai, COM(2015) 192 final, 2015. gada 6. maijs.
([5]) COM(2016) 176 final, 2016. gada 19. aprīlis.
([6]) COM(2011) 311 galīgā redakcija, 2011. gada 1. jūnijs.

(6) Lēmums par IKT specifikācijas noteikšanu jāpieņem pēc apspriešanās ar Eiropas daudzpusējo ieinteresēto personu forumu IKT standartizācijas jautājumos, kas izveidots ar Komisijas Lēmumu 2011/C 349/04 ([1]), un citādām konsultācijām ar nozares ekspertiem.

(7) Eiropas daudzpusējais ieinteresēto personu forums IKT standartizācijas jautājumos izvērtēja un deva pozitīvu atzinumu par iespēju publiskajos iepirkumos atsaukties uz šādām tehniskajām specifikācijām: "*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*") un "*DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security*" ("*DANE-SMTP*"), ko izstrādājusi Interneta tehniskā uzdevumgrupa (*IETF*), un "*Structured Threat Information Expression*" ("*STIX 1.2*") un "*Trusted Automated Exchange of Indicator Information*" ("*TAXII 1.1*"), ko izstrādājusi Strukturētas informācijas standartu veicināšanas organizācija (*OASIS*). Foruma sniegtais novērtējums un atzinums tad tika iesniegts apspriešanai nozares ekspertiem, kuri apstiprināja pozitīvo atzinumu par iespēju atsaukties uz minētajām tehniskajām specifikācijām.

(8) *IETF* izstrādātā tehniskā specifikācija "SPF" ir atvērts standarts, kas norāda tehnisko metodi, ar kuru konstatē sūtītāja adreses falsifikāciju. SPF piedāvā iespēju pārbaudīt, vai ziņa tiek sūtīta no servera, kas ir autorizēts to darīt. Tā ir vienkārša e-pastu validēšanas sistēma, kura ir izstrādāta, lai atklātu e-pastu viltošanu, un kura nodrošina mehānismu, kas ļauj saņemt tā saucamos MX ierakstus, lai tādējādi pārbaudītu, vai no domēna ienākošais e-pasts nāk no hostdatora, kuram ir minētā domēna administratoru autorizējums. SPF nolūks ir novērst tādu mēstuļu saņemšanu, kurām ir viltotas sūtītāju adreses no konkrētā domēna. Saņēmēji var pārbaudīt SPF ierakstus, lai noteiktu, vai ziņa, kas šķietami nāk no minētā domēna, ir sūtīta no autorizēta e-pastu servera.

(9) *IETF* izstrādātā *STARTTLS-SMTP* ir veids, kā pastāvošo nedrošo savienojumu pārveidot par drošu savienojumu. *STARTTLS* ir vienkāršā pasta pārsūtīšanas protokola (*SMTP*) paplašinājums, kas ļauj *SMTP* serverim un klientam izmantot transporta slāņa drošību (*TLS*), lai nodrošinātu privātu, autentificētu saziņu internetā. Tieši nedrošā e-pasta saziņa ir galvenais uzbrukuma mērķis, īstenojot kiberuzbrukumus valdības komunikācijas tīkliem. Ja lietotājs nosūta e-pastu, lietotāja pasta pakalpojumu nodrošinātāja pasta serveris sūtīs šo e-pastu saņēmēja pasta serverim. Pirms tam savienojumu starp šiem pasta serveriem var padarīt drošu, izmantojot *TLS*. *STARTTLS* piedāvā veidu, kā nešifrētu (vienkārša teksta) savienojumu pārveidot par šifrētu *TLS* savienojumu.

(10) *IETF* izstrādātā *DANE-SMTP* ir protokolu virkne, ar kuru paaugstina interneta drošību, ļaujot domēna nosaukumu sistēmā (*DNS*) ievietot atslēgas, kas aizsargātas ar *DNSSEC* ("*DNS Security*"). Kad tiek veidots drošs savienojums ar nezināmu pusi, ir vēlama tiešsaistes pārbaude par sūtītājas puses autentiskumu un par galamērķi. To var izdarīt, izmantojot sertifikātus, kurus izdod *PKI* sistēmai piederīgas sertifikācijas iestādes, vai ar pašparakstītiem sertifikātiem. *DANE* ļauj domēna vārda īpašniekam ("reģistrētājam") sniegt papildinformāciju papildus tiešsaistes sertifikātiem, izmantojot ar *DNSSEC* aizsargātus *DNS* ierakstus. Tādējādi *DANE* ir īpaši svarīga aktīvu uzbrucēju atvairīšanai.

(11) *OASIS* izstrādātā *STIX 1.2* ir valoda, ar kuru standartizētā un strukturētā veidā apraksta kiberdraudu informāciju. Tā aptver galvenos tematus kiberdraudu datu jomā, atvieglojot analīzi un informācijas apmaiņu par uzbrukumiem. Tā raksturo plašu kiberdraudu informācijas kopumu, kurā iekļauti pretinieku darbības indikatori, tādi kā IP adreses un datņu jaucējvērtības, un kontekstuāla informācija par draudiem, tāda kā pretinieka taktika, tehnika un procedūras (*TTP*), ekspluatācijas mērķi, kampaņas un rīcības virzieni (*COA*). Šīs informācijas kopums pilnībā raksturo kiberuzbrucēja motīvus, spējas un darbības un tādējādi palīdz aizsargāties pret uzbrukumiem.

(12) Cita *OASIS* izstrādāta tehniskā specifikācija, *TAXII v1.1*, standartizē kiberdraudu informācijas uzticamo, automatizēto apmaiņu. *TAXII* definē pakalpojumus un ziņu apmaiņu, lai dalītos ar tādu kiberdraudu informāciju pāri organizācijas, produkta vai pakalpojuma robežām, kura rada nepieciešamību rīkoties, lai atklātu, novērstu un mazinātu kiberdraudus. *TAXII* dod iespēju organizācijām panākt labāku situācijas izpratni attiecībā uz jauniem draudiem un ļauj tām ērti dalīties informācijā ar partneriem, tādējādi uzlabojot pastāvošās attiecības un sistēmas,

([1]) Komisijas 2011. gada 28. novembra Lēmums 2011/C 349/04, ar ko izveido Eiropas daudzpusēju ieinteresēto personu forumu par IKT standartizāciju (OV C 349, 30.11.2011., 4. lpp.).

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Publiskajā iepirkumā var atsaukties uz pielikumā uzskaitītajām tehniskajām specifikācijām.

2. pants

Šis lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2017. gada 11. decembrī

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER

PIELIKUMS

Interneta tehniskā uzdevumgrupa (*IETF*)

Nr.	IKT tehniskās specifikācijas nosaukums
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)*

Strukturēto informācijas standartu veicināšanas organizācija (*OASIS*)

Nr.	IKT tehniskās specifikācijas nosaukums
1.	*STIX 1.2 Structured Threat Information Expression*
2.	*TAXII 1.1 Trusted Automated Exchange of Indicator Information*