UITVOERINGSBESLUIT (EU) 2017/2288 VAN DE COMMISSIE

van 11 december 2017

betreffende de vaststelling van technische ICT-specificaties als referenties bij overheidsopdrachten

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad ([1]), en met name artikel 13, lid 1,

Na raadpleging van het Europees multistakeholderplatform inzake ICT-normalisatie en van deskundigen uit de bedrijfstak,

Overwegende hetgeen volgt:

(1) Normalisatie speelt een belangrijke rol bij de ondersteuning van de Europa 2020-strategie ([2]). In verschillende vlaggenschipinitiatieven van de Europa 2020-strategie is op het belang van vrijwillige normalisatie op de markten voor producten en diensten gewezen om de compatibiliteit en interoperabiliteit tussen producten en diensten te kunnen waarborgen, technologische ontwikkelingen te kunnen stimuleren en innovatie te kunnen ondersteunen.

(2) Normen zijn essentieel voor het Europese concurrentievermogen en van cruciaal belang voor innovatie en vooruitgang. In de mededelingen van de Commissie over de eengemaakte markt ([3]) en de digitale eengemaakte markt ([4]) is bevestigd dat gemeenschappelijke normen belangrijk zijn om te waarborgen dat de netwerken en systemen in de Europese digitale economie voldoende interoperabel zijn. Dit is kracht bijgezet door de goedkeuring van de mededeling over normalisatieprioriteiten op ICT-gebied ([5]), waarin de Commissie heeft aangegeven voor welke prioritaire ICT-technologieën normalisatie van cruciaal belang wordt geacht voor de voltooiing van de digitale eengemaakte markt.

(3) In de mededeling van de Commissie „Een strategische visie voor Europese normen: de duurzame groei van de Europese economie tussen nu en 2020 bevorderen en versnellen" ([6]) worden de specifieke omstandigheden van de normalisatie van informatie- en communicatietechnologieën (ICT) erkend, waarbij oplossingen, toepassingen en diensten vaak worden ontwikkeld door wereldwijde ICT-fora en -consortia die zich tot leidende organisaties voor de ontwikkeling van ICT-normen hebben ontpopt.

(4) Bij Verordening (EU) nr. 1025/2012 betreffende Europese normalisatie is een systeem opgezet waarbij de Commissie kan besluiten tot vaststelling van de relevantste en meest algemeen aanvaarde technische ICT-specificaties die zijn vastgesteld door organisaties die geen Europese, internationale of nationale normalisatieorganisaties zijn, die vervolgens kunnen worden gebruikt als referentie, vooral om interoperabiliteit mogelijk te maken, bij overheidsopdrachten. De mogelijkheid om bij de aankoop van hardware, software en informatietechnologiediensten het volledige scala van technische ICT-specificaties te gebruiken, maakt interoperabiliteit tussen apparatuur, diensten en toepassingen mogelijk, helpt voorkomen dat overheidsdiensten aan een bepaalde technologie gebonden zijn en na het aflopen van een aanbestedingscontract niet op een andere aanbieder kunnen overstappen doordat merkgebonden ICT-oplossingen zijn gebruikt, en bevordert de concurrentie bij de levering van interoperabele ICT-oplossingen.

(5) Om als referentie bij overheidsopdrachten in aanmerking te komen, moeten technische ICT-specificaties voldoen aan de voorschriften van bijlage II bij Verordening (EU) nr. 1025/2012. Het voldoen aan deze voorschriften geeft de overheden de zekerheid dat de technische ICT-specificaties zijn vastgesteld in overeenstemming met de beginselen van openheid, transparantie, onpartijdigheid en consensus die op het gebied van normalisatie door de Wereldhandelsorganisatie zijn erkend.

([1]) PB L 316 van 14.11.2012, blz. 12.
([2]) Mededeling van de Commissie „EUROPA 2020 — Een strategie voor slimme, duurzame en inclusieve groei", COM(2010) 2020 definitief van 3 maart 2010.
([3]) Mededeling van de Commissie „De eengemaakte markt verbeteren: meer mogelijkheden voor mensen en ondernemingen", COM(2015) 550 final van 28 oktober 2015.
([4]) Mededeling over een strategie voor een digitale eengemaakte markt voor Europa, COM(2015) 192 final van 6 mei 2015.
([5]) COM(2016) 176 final van 19 april 2016.
([6]) COM(2011) 311 definitief van 1 juni 2011.

(6) Het besluit om een ICT-specificatie vast te stellen, moet worden goedgekeurd na raadpleging van het Europees multistakeholderplatform inzake ICT-normalisatie, dat is opgericht bij Besluit 2011/C 349/04 van de Commissie ([1]), aangevuld met andere vormen van raadpleging van deskundigen uit de bedrijfstak.

(7) Het Europees multistakeholderplatform inzake ICT-normalisatie heeft de volgende technische specificaties voor gebruik als referentie bij overheidsopdrachten geëvalueerd en daarover een positief advies uitgebracht: „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) en „DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security" (DANE- SMTP), ontwikkeld door de Internet Engineering Task Force (IETF), en „Structured Threat Information Expression" (STIX 1.2) en „Trusted Automated Exchange of Indicator Information" (TAXII 1.1), ontwikkeld door de Organization for the Advancement of Structured Information Standards (OASIS). De evaluatie en het advies van het platform zijn vervolgens ter raadpleging aan deskundigen uit de bedrijfstak voorgelegd, die het positieve advies over de vaststelling hebben onderschreven.

(8) De door de IETF ontwikkelde technische specificatie SPF is een open standaard die een technische methode specificeert voor de opsporing van afzendervervalsing. SPF biedt de mogelijkheid om te controleren of een bericht is verzonden vanaf een server die daartoe gemachtigd is. Het is een eenvoudig e-mailvalidatiesysteem dat bedoeld is om e-mailspoofing op te sporen met behulp van een mechanisme waarmee ontvangende mailservers kunnen controleren of inkomende e-mails die uit een domein lijken te komen, afkomstig zijn van een host die daartoe door de beheerders van dat domein is gemachtigd. SPF is bedoeld om te voorkomen dat spammers e-mails met valse afzenderadressen in een bepaald domein kunnen verzenden. De ontvangers kunnen in een SPF-bestand nagaan of een bericht dat uit dat domein lijkt te komen, van een daartoe gemachtigde mailserver afkomstig is.

(9) STARTTLS-SMTP, dat door de IETF is ontwikkeld, is een manier om een bestaande onveilige verbinding op te waarderen tot een veilige verbinding. STARTTLS vormt een aanvulling op het Simple Mail Transfer Protocol (SMTP), waardoor servers en clients die het SMTP toepassen, Transport Layer Security (TLS) kunnen gebruiken voor vertrouwelijke, geauthenticeerde communicatie via internet. Met name onbeveiligd e-mailverkeer vormt een belangrijke aanvalsvector voor het binnendringen van overheidsnetwerken. Als een gebruiker een e-mailbericht verstuurt, zendt de mailserver van de provider van de gebruiker dat bericht naar de mailserver van de ontvanger. De verbinding tussen deze mailservers kan vooraf worden beveiligd met TLS. Met STARTTLS kan een niet-versleutelde verbinding (platte tekst) worden opgewaardeerd tot een versleutelde TLS-verbinding.

(10) DANE-SMT, dat door de IETF is ontwikkeld, is een verzameling protocollen om de internetbeveiliging te verbeteren door het mogelijk te maken sleutels op te nemen in het Domain Name System (DNS) en te beveiligen met DNSSEC (DNS Security). Het is wenselijk dat bij de totstandbrenging van een beveiligde verbinding met een onbekende de authenticiteit van de verzender en de geadresseerde online wordt gecontroleerd. Dit kan met behulp van certificaten die binnen het PKI-systeem door een certificaatautoriteit zijn uitgegeven of met behulp van zelf ondertekende certificaten. DANE geeft de domeinhouder (de registrant) de mogelijkheid de onlinecertificaten aan te vullen met extra informatie, via een met DNSSEC beveiligd DNS-bestand. Daarom is DANE zeer belangrijk om actieve aanvallers te bestrijden.

(11) STIX 1.2, dat door OASIS is ontwikkeld, is een taal om informatie over cyberbedreigingen op gestandaardiseerde en gestructureerde wijze te beschrijven. Deze taal bestrijkt de belangrijkste cyberbedreigingsaspecten en vereenvoudigt de analyse en uitwisseling van informatie over aanvallen. In deze taal kan een uitgebreide reeks cyberbedreigingsgegevens worden gekarakteriseerd, zoals indicatoren van vijandelijke activiteit (bv. IP-adressen en hashes van bestanden) en contextuele informatie over bedreigingen (bv. vijandelijke tactieken, technieken en procedures (TTP's), exploitatiedoelwitten, campagnes en handelswijzen (Courses of Action; COA's)). Al deze informatie bij elkaar karakteriseert de beweegredenen, de capaciteiten en de activiteiten van de cybervijand, waardoor zij bijdraagt tot het afslaan van aanvallen.

(12) De technische specificatie TAXII v1.1, die ook door OASIS is ontwikkeld, maakt het mogelijk op gestandaardiseerde en betrouwbare wijze automatisch informatie over cyberbedreigingen uit te wisselen. TAXII specificeert diensten en berichtenuitwisseling waarmee bruikbare informatie over cyberbedreigingen tussen verschillende organisaties, producten of diensten kan worden gedeeld om cyberbedreigingen op te sporen, te voorkomen en te beteugelen. TAXII biedt organisaties de mogelijkheid zich een beter beeld van opkomende bedreigingen te vormen en gemakkelijk informatie uit te wisselen met partners, terwijl zij tegelijkertijd meer voordeel uit de bestaande relaties en systemen kunnen halen,

([1]) Besluit 2011/C 349/04 van de Commissie van 28 november 2011 tot oprichting van een Europees multistakeholderplatform inzake ICT-normalisatie (PB C 349 van 30.11.2011, blz. 4).

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

De in de bijlage vermelde technische specificaties komen in aanmerking om bij overheidsopdrachten als referentie te dienen.

Artikel 2

Dit besluit treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Gedaan te Brussel, 11 december 2017.

Voor de Commissie
De voorzitter
Jean-Claude JUNCKER

BIJLAGE

Internet Engineering Task Force (IETF)

Nr.	Naam van technische ICT-specificatie
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.	Naam van technische ICT-specificatie
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information