DÉCISION D'EXÉCUTION (UE) 2017/2288 DE LA COMMISSION

du 11 décembre 2017

relative à l'identification des spécifications techniques des TIC pouvant servir de référence dans la passation des marchés publics

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil ([1]), et notamment son article 13, paragraphe 1,

après consultation de la plateforme européenne pluripartite sur la normalisation des TIC ainsi que des experts du secteur,

considérant ce qui suit:

(1) La normalisation joue un rôle important à l'appui de la stratégie Europe 2020 ([2]). Plusieurs initiatives phares de la stratégie Europe 2020 ont souligné l'importance de la normalisation volontaire dans les marchés de produits ou de services pour garantir la compatibilité et l'interopérabilité des produits et des services, favoriser le développement technologique et soutenir l'innovation.

(2) Les normes sont essentielles à la compétitivité européenne et indispensables aux fins de l'innovation et du progrès. Les communications de la Commission sur le marché unique ([3]) et le marché unique numérique ([4]) confirment l'importance de normes communes en vue de garantir l'interopérabilité des réseaux et des systèmes nécessaire à l'économie numérique européenne. Ce rôle est renforcé par l'adoption de la communication sur les priorités pour la normalisation en matière de TIC ([5]), dans laquelle la Commission définit les technologies TIC prioritaires pour lesquelles la normalisation est considérée comme essentielle à l'achèvement du marché unique numérique.

(3) La communication de la Commission intitulée «Une vision stratégique pour les normes européennes: aller de l'avant pour améliorer et accélérer la croissance durable de l'économie européenne à l'horizon 2020» ([6]) a reconnu la spécificité de la normalisation dans le domaine des technologies de l'information et de la communication (TIC), où les solutions, applications et services sont souvent élaborés par des instances et consortiums mondiaux du secteur des TIC qui sont désormais des organisations de référence en matière d'élaboration de normes dans ce domaine.

(4) Le règlement (UE) nº 1025/2012 sur la normalisation européenne a établi un système dans lequel la Commission peut décider d'identifier les spécifications techniques des TIC les plus pertinentes et les plus largement acceptées émanant d'organisations qui ne sont pas des organisations de normalisation européennes, internationales ou nationales, qui peuvent être référencées, essentiellement pour permettre l'interopérabilité dans la passation des marchés publics. La possibilité de recourir à l'ensemble des spécifications techniques des TIC lors de l'achat de matériel, de logiciels et de services informatiques permettra de garantir l'interopérabilité entre appareils, services et applications, d'éviter que les administrations publiques ne deviennent des clients captifs, du fait qu'elles utilisent dans le domaine des TIC des solutions propriétaires ne leur permettant pas de changer de fournisseur à la fin du marché public ainsi que de favoriser la concurrence dans la fourniture de solutions interopérables dans le domaine des TIC.

(5) Les spécifications techniques des TIC peuvent servir de référence dans la passation des marchés publics, à condition qu'elles soient conformes aux exigences énoncées à l'annexe II du règlement (UE) nº 1025/2012. Le respect de ces exigences garantit aux autorités publiques que les spécifications techniques des TIC sont établies conformément aux principes d'ouverture, de transparence, d'impartialité et de consensus reconnus par l'Organisation mondiale du commerce dans le domaine de la normalisation.

([1]) JO L 316 du 14.11.2012, p. 12.
([2]) Communication de la Commission intitulée «Europe 2020 — Une stratégie pour une croissance intelligente, durable et inclusive». COM(2010) 2020 final du 3 mars 2010.
([3]) Communication de la Commission intitulée «Améliorer le marché unique: de nouvelles opportunités pour les citoyens et les entreprises». COM(2015) 550 final du 28 octobre 2015.
([4]) Communication intitulée «Stratégie pour un marché unique numérique en Europe». COM(2015) 192 final du 6 mai 2015.
([5]) COM(2016) 176 final du 19 avril 2016.
([6]) COM(2011) 311 final du 1er juin 2011.

(6) Avant d'être adoptée, toute décision d'identifier une spécification dans le domaine des TIC doit faire l'objet d'une consultation de la plateforme européenne pluripartite sur la normalisation des TIC créée par la décision 2011/C 349/04 de la Commission ([1]), complétée par d'autres formes de consultation des experts du secteur.

(7) La plateforme européenne pluripartite sur la normalisation des TIC a procédé à une évaluation et a rendu un avis positif en ce qui concerne l'identification des spécifications techniques suivantes pouvant servir de référence dans la passation des marchés publics: «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)» et «DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security ('DANE- SMTP)», développées par l'Internet Engineering Task Force (IETF); «Structured Threat Information Expression (STIX 1.2)» et «Trusted Automated Exchange of Indicator Information (TAXII 1.1)», développée par l'Organisation pour l'avancement des normes relatives aux informations structurées (OASIS). L'évaluation réalisée par la plateforme et l'avis émis par cette dernière ont ensuite été soumis pour consultation aux experts du secteur, qui se sont eux aussi prononcés en faveur de l'identification en question.

(8) La spécification technique «SPF» développée par l'IETF est une norme ouverte qui définit une méthode technique permettant de détecter les falsifications d'adresse de l'expéditeur. La SPF offre l'option de vérifier si un message est envoyé à partir d'un serveur qui est autorisé à le faire. Il s'agit simplement d'un système de validation des courriers électroniques permettant de détecter les usurpations d'adresse électronique (spoofing) en fournissant un mécanisme permettant au destinataire d'un courrier électronique de vérifier que le courrier provenant d'un domaine a bien été émis par un hôte autorisé par les administrateurs de ce domaine. La FPS a pour but d'empêcher les spammeurs d'envoyer des messages à un domaine précis avec de fausses adresses de provenance. Les destinataires peuvent se référer à un enregistrement SPF pour déterminer si un message prétendant provenir de ce domaine provient d'un serveur de messagerie autorisé.

(9) «STARTTLS-SMTP», développée par l'IETF, permet de transformer une connexion existante non sécurisée en une connexion sécurisée. STARTTLS est une extension du service «Simple Mail Transfer Protocol (protocole SMTP)» qui permet à un serveur et client SMTP d'utiliser le Transport Layer Security (TLS) pour remettre des courriers privés et authentifiés par Internet. Des courriers électroniques non sécurisés sont un important vecteur d'attaque pour les réseaux des autorités publiques. Lorsqu'un utilisateur envoie un courrier électronique, le serveur de messagerie entrant enverra ce courrier électronique au serveur de messagerie sortant. La connexion entre ces serveurs de messagerie peut être sécurisée au préalable avec la TLS. STARTTLS offre un moyen de prendre une connexion non chiffrée (texte simple) et de la mettre à jour vers une connexion chiffrée en utilisant TLS.

(10) «DANE-SMTP», développée par IETF, est une série de protocoles servant à renforcer la sécurité d'Internet en permettant l'introduction de clés dans le «Domain Name System» (DNS) et leur sécurisation par le protocole DNSSEC («DNS»). Lors de la mise en place d'une connexion sécurisée avec un tiers inconnu, une vérification en ligne de l'authenticité de l'expéditeur et du destinataire est souhaitable. Cela peut se faire au moyen de certificats délivrés par des autorités de certification («AC») dans le système PKI ou au moyen de certificats auto-signés. DANE permet au titulaire d'un domaine («enregistrant») de fournir des informations supplémentaires en plus des certificats en ligne au moyen d'un enregistrement DNS sécurisé par le protocole DNSSEC. DANE est donc particulièrement importante pour lutter contre les attaquants actifs.

(11) «STIX 1.2», développée par OASIS, est un langage pour décrire de manière normalisée et structurée les informations sur les cyber-menaces. Elle couvre d'importants sujets en matière de données relatives aux cyber-menaces, en facilitant l'analyse et l'échange au sujet des cyber-attaques. Elle contient un vaste ensemble d'informations sur les cyber-menaces, y compris des indicateurs d'activité malveillante, telles que les adresses IP et les empreintes numériques ainsi que des informations contextuelles concernant des menaces telles que les tactiques, les techniques et les procédures (TTP); sur les objectifs d'exploitation, les campagnes et les moyens d'action (COA). Ensemble, ces informations permettent de définir les motivations de la cyber-attaque, ses capacités et ses activités, et de contribuer ainsi à la défense contre ces attaques.

(12) La spécification technique «TAXII v1.1», développée par OASIS, normalise l'échange automatisé et sécurisé d'informations sur les cyber-menaces. TAXII définit les services et les échanges de messages pour le partage d'informations liées aux cyber-menaces entre organisations, produits ou services en vue de la détection, de la prévention et de l'atténuation des cyber-menaces. TAXII permet aux organisations d'avoir une meilleure connaissance de la situation en matière de menaces émergentes et d'aisément échanger des informations avec des partenaires, tout en exploitant les liens et systèmes existants,

([1]) Décision 2011/C 349/04 de la Commission du 28 novembre 2011 portant création d'une plateforme européenne pluripartite sur la normalisation des TIC (JO C 349 du 30.11.2011, p. 4).

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Les spécifications techniques énumérées en annexe peuvent servir de référence dans la passation des marchés publics.

Article 2

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 11 décembre 2017.

Par la Commission
Le président
Jean-Claude JUNCKER

ANNEXE

Internet Engineering Task Force (IETF)

Non	Intitulé de la spécification technique des 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)

Organisation pour l'avancement des normes structurées de l'information (OASIS)

Non	Intitulé de la spécification technique des TIC
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information