DECISÃO DE EXECUÇÃO (UE) 2017/2288 DA COMISSÃO

de 11 de dezembro de 2017

relativa à identificação das Especificações Técnicas das TIC para referência nos contratos públicos

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho ([1]), nomeadamente o artigo' 13.º, n.º 1,

Após consulta da plataforma multilateral europeia sobre a normalização no domínio das TIC e dos peritos do setor,

Considerando o seguinte:

(1) A normalização desempenha um papel importante no apoio à estratégia Europa 2020 ([2]). Várias iniciativas emblemáticas da estratégia Europa 2020 sublinham a importância de uma normalização voluntária nos mercados dos produtos ou serviços, a fim de garantir a compatibilidade e a interoperabilidade entre produtos e serviços, promover o desenvolvimento tecnológico e apoiar a inovação.

(2) As normas são essenciais para a competitividade europeia e indispensáveis para a inovação e o progresso. As comunicações da Comissão sobre o mercado único ([3]) e o mercado único digital ([4]) confirmam quão importante é a existência de normas comuns para garantir a interoperabilidade das redes e dos sistemas da Economia Digital Europeia. Esta perspetiva foi reforçada com a adoção da Comunicação sobre as prioridades de normalização no domínio das TIC ([5]), na qual a Comissão identifica tecnologias prioritárias no domínio das TIC em que a normalização é considerada essencial para a conclusão do mercado único digital.

(3) A Comunicação da Comissão intitulada «Uma visão estratégica para a normalização europeia: reforçar e acelerar o crescimento sustentável da economia europeia até 2020» ([6]) reconhece a especificidade da normalização no domínio das tecnologias da informação e comunicação (TIC), em que as soluções, as aplicações e os serviços são muitas vezes desenvolvidos por fóruns e consórcios globais deste setor que emergiram como organismos de vanguarda na elaboração de normas para as TIC.

(4) O Regulamento (UE) n.º 1025/2012 relativo à normalização europeia estabelece um sistema graças ao qual a Comissão pode decidir identificar as especificações técnicas mais pertinentes e mais amplamente aceites no domínio das TIC, emitidas por organismos que não são organismos de normalização europeus, internacionais ou nacionais que poderão em seguida ser referenciados, essencialmente para permitir a interoperabilidade na contratação pública. A possibilidade de utilizar todo o acervo de especificações técnicas das TIC ao adquirir *hardware*, *software* e serviços no domínio das tecnologias da informação não só assegurará a interoperabilidade entre dispositivos, serviços e aplicações, como ajudará as administrações públicas a evitar situações de dependência (resultantes do facto de a entidade pública adjudicante não poder mudar de fornecedor após o termo do contrato por utilizar soluções TIC proprietárias) e incentivará a concorrência a oferecer soluções TIC interoperáveis.

(5) Para poderem ser elegíveis para efeitos de referência nos contratos públicos, as especificações técnicas das TIC têm de cumprir os requisitos estabelecidos no anexo II do Regulamento (UE) n.º 1025/2012. O cumprimento desses requisitos garante às autoridades públicas que as especificações técnicas das TIC foram estabelecidas em conformidade com os princípios de abertura, transparência, imparcialidade e consenso reconhecidos pela Organização Mundial do Comércio no domínio da normalização.

([1]) JO L 316 de 14.11.2012, p. 12.
([2]) Comunicação da Comissão «Europa 2020. Estratégia para um crescimento inteligente, sustentável e inclusivo». COM(2010) 2020 final, de 3 de março de 2010.
([3]) Comunicação da Comissão «Melhorar o Mercado Único: mais oportunidades para os cidadãos e as empresas». COM(2015) 550 final, de 28 de outubro de 2015.
([4]) Comunicação sobre uma Estratégia para o Mercado Único Digital da Europa. COM(2015) 192 final, de 6 de maio de 2015.
([5]) COM(2016) 176 final, de 19 de abril de 2016.
([6]) COM(2011) 311 final, de 1 de junho de 2011.

(6) As decisões de identificação de uma especificação TIC devem ser adotadas após consulta da plataforma multilateral europeia sobre a normalização no domínio das TIC, criada pela Decisão 2011/C 349/04 da Comissão ([1]), complementada por outras formas de consulta dos peritos do setor.

(7) A plataforma multilateral europeia sobre a normalização no domínio das TIC avaliou e emitiu um parecer favorável sobre a identificação das seguintes especificações técnicas para referência nos contratos públicos: «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)» e «DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (DANE- SMTP)» desenvolvida pelo Grupo de Missão de Engenharia da Internet (IETF); «Structured Threat Information Expression (STIX 1.2)» e «Trusted Automated Exchange of Indicator Information (TAXII 1.1)» desenvolvidos pela Organização para o Avanço de Normas de Informação Estruturadas («OASIS»). A avaliação e o parecer da plataforma foram posteriormente objeto de consulta aos peritos do setor, que confirmaram o parecer favorável sobre a sua identificação.

(8) A especificação técnica «SPF», desenvolvida pelo IETF, é uma norma aberta que especifica um método técnico para detetar as falsificações do endereço do remetente. A SPF oferece a opção de verificar se uma mensagem é enviada de um servidor autorizado a fazê-lo. Trata-se de um sistema simples de validação de mensagens de correio eletrónico que permite detetar usurpações de endereços (spoofing), fornecendo um mecanismo que permite ao destinatário de uma mensagem verificar que a mensagem que provém de um dado domínio é remetida de um anfitrião autorizado pelos administradores desse domínio. O objetivo do SPF é impedir os «spammers» de enviar mensagens com endereços de remetentes falsos num determinado domínio. Os destinatários podem recorrer a um registo SPF para determinar se uma mensagem alegadamente proveniente desse domínio provém de um servidor de correio autorizado.

(9) «STARTTLS-SMTP», desenvolvido pelo IETF, é uma forma de fazer com que uma ligação existente não segura seja convertida numa ligação segura. STARTTLS é uma extensão do serviço Simple Mail Transfer Protocol (SMTP) que permite a um servidor e a um cliente SMTP usar o Transport Layer Security («TLS») para fornecer comunicação privada e autenticada através da Internet. São principalmente as comunicações por correio eletrónico não seguras que constituem um importante vetor de intrusão nas redes das administrações públicas. Se um utilizador enviar uma mensagem de correio eletrónico, o servidor de correio do utilizador enviará esta mensagem de correio eletrónico para o servidor de correio do destinatário. A conexão entre os servidores de correio eletrónico pode ser tornada segura de antemão com TLS. STARTTLS oferece a possibilidade de mudar uma conexão não encriptada (texto simples) passando-a para conexão TLS encriptada.

(10) «DANE-SMTP», desenvolvido pelo IETF, é um conjunto de protocolos que servem para reforçar a segurança da Internet, ao permitir a introdução de chaves no Domain Name System (DNS) e a sua securitização por DNSSEC (DNS Security). Ao estabelecer uma conexão segura com uma parte desconhecida, é desejável que haja uma verificação em linha da autenticidade do remetente e do destinatário. Essa verificação pode ser feita por meio de certificados emitidos pelas autoridades de certificação (AC) no seio do sistema PKI, ou por certificados autoassinados. DANE permite ao titular de um domínio («registante»), fornecer informações adicionais para além dos certificados em linha por meio de um registo DNS securitizado pelo protocolo DNSSEC. DANE é, portanto, particularmente importante para combater os atacantes ativos.

(11) «STIX 1.2», desenvolvida pela OASIS, é uma linguagem para descrever informações sobre ciberameaças, de forma estruturada e normalizada. Cobre temas fundamentais relacionados com dados sobre ciberameaças, facilitando a análise e o intercâmbio sobre os ataques. Caracteriza um vasto conjunto informações sobre ciberameaças, incluindo indicadores de atividades adversas, como sejam endereços IP e impressões numéricas dos ficheiros, assim como informações contextuais sobre ameaças como sejam «Tactics, Techniques and Procedures (TTP)»; alvos de exploração; campanhas e meios de ação (COA). Em conjunto, estas informações permitem descrever cabalmente as motivações, as capacidades e as atividades dos ciberadversários e, assim, ajudar na defesa contra os ataques.

(12) A «Especificação técnica TAXII v1.1», também desenvolvida pela OASIS, normaliza o intercâmbio automatizado de informações sobre ciberameaças. A TAXII define serviços e trocas de mensagens para a partilha de informações sobre ciberameaças entre organizações, produtos ou serviços, tendo em vista a deteção, a prevenção e a mitigação das ciberameaças. A TAXII permite às organizações ter uma melhor consciência da situação respeitante às ameaças emergentes e facilmente partilhar informações com os parceiros, melhorando ao mesmo tempo os sistemas e as relações existentes,

([1]) Decisão 2011/C 349/04 da Comissão, de 28 de novembro de 2011, que institui a plataforma multilateral europeia sobre a normalização no domínio das TIC (JO C 349 de 30.11.2011, p. 4).

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

As especificações técnicas constantes do anexo são elegíveis para referência nos contratos públicos.

Artigo 2.º

A presente decisão entra em vigor no vigésimo dia subsequente ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 11 de dezembro de 2017.

Pela Comissão
O Presidente
Jean-Claude JUNCKER

ANEXO

Grupo de Missão de Engenharia da Internet (IETF)

N.º	Título das especificações técnicas das 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)

Organização para o Aprofundamento de Normas de Informação Estruturadas (OASIS)

N.º	Título das especificações técnicas das TIC
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information