DURCHFÜHRUNGSBESCHLUSS (EU) 2017/2288 DER KOMMISSION

vom 11. Dezember 2017

zur Festlegung der technischen Spezifikationen im IKT-Bereich, auf die bei der Vergabe öffentlicher Aufträge Bezug genommen werden kann

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates [1], insbesondere auf Artikel 13 Absatz 1,

nach Konsultation der Europäischen Multi-Stakeholder-Plattform für die IKT-Normung und der Sachverständigen des Sektors,

in Erwägung nachstehender Gründe:

(1) Die Normung leistet einen wichtigen Beitrag zur Unterstützung der Strategie „Europa 2020“ [2]. Wie in mehreren Leitinitiativen der Strategie „Europa 2020“ betont wurde, spielt die freiwillige Normung auf den Waren- und Dienstleistungsmärkten eine wichtige Rolle, wenn es darum geht, die Kompatibilität und Interoperabilität von Produkten und Dienstleistungen zu gewährleisten und die technologische Entwicklung und die Innovation zu fördern.

(2) Normen sind von zentraler Bedeutung für die Wettbewerbsfähigkeit Europas sowie für Innovation und Fortschritt. In den Mitteilungen der Kommission über den Binnenmarkt [3] und den digitalen Binnenmarkt [4] wird bestätigt, wie wichtig gemeinsame Normen dafür sind, die erforderliche Interoperabilität von Netzwerken und Systemen in der europäischen digitalen Wirtschaft zu gewährleisten. Mit der Annahme der Mitteilung über Schwerpunkte der IKT-Normung für den digitalen Binnenmarkt [5] hat sich dies bestätigt; darin nennt die Kommission vorrangige IKT-Technologien, in denen die Normung als entscheidender Faktor für die Vollendung des digitalen Binnenmarkts angesehen wird.

(3) Die Kommission hat in ihrer Mitteilung „Eine strategische Vision der europäischen Normung: Weitere Schritte zur Stärkung und Beschleunigung des nachhaltigen Wachstums der europäischen Wirtschaft bis zum Jahr 2020“ [6] die Besonderheit der Normung im Bereich der Informations- und Kommunikationstechnologien (IKT) anerkannt, wo einschlägige Lösungen, Anwendungen und Dienste häufig von globalen IKT-Foren und -Vereinigungen entwickelt werden, die heute eine Führungsrolle bei der Entwicklung von IKT-Normen einnehmen.

(4) Durch die Verordnung (EU) Nr. 1025/2012 zur europäischen Normung wurde ein System eingeführt, mit dem die Kommission festlegen kann, welche technischen Spezifikationen im IKT-Bereich, die nicht von europäischen, internationalen oder nationalen Normungsgremien erarbeitet wurden, die größte Relevanz und die breiteste Akzeptanz haben; auf diese kann dann Bezug genommen werden, in erster Linie, um Interoperabilität bei der Vergabe öffentlicher Aufträge zu gewährleisten. Wenn die Möglichkeit besteht, die gesamte Bandbreite von technischen Spezifikationen im IKT-Bereich bei der Beschaffung von Hardware, Software und IT-Dienstleistungen zu nutzen, wird die Interoperabilität zwischen Geräten, Diensten und Anwendungen gesichert, die Bindung öffentlicher Auftraggeber an einen einzigen Anbieter vermieden — die zustande kommt, wenn der öffentliche Auftraggeber den Anbieter nach Vertragsablauf nicht wechseln kann, da proprietäre IKT-Lösungen verwendet wurden — und der Wettbewerb bei der Lieferung interoperabler IKT-Lösungen angekurbelt.

(5) Damit bei der Vergabe öffentlicher Aufträge auf bestimmte technische IKT-Spezifikationen Bezug genommen werden kann, müssen diese die Anforderungen des Anhangs II der Verordnung (EU) Nr. 1025/2012 erfüllen. Bei technischen Spezifikationen für IKT, die diese Anforderungen erfüllen, können die öffentlichen Auftraggeber mit Gewissheit davon ausgehen, dass sie im Einklang mit den von der Welthandelsorganisation auf dem Gebiet der Normung anerkannten Grundsätzen der Offenheit, der Transparenz, der Unparteilichkeit und des Konsens erstellt wurden.

---

[1] ABl. L 316 vom 14.11.2012, S. 12.
[2] Mitteilung der Kommission mit dem Titel „Europa 2020 — Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum“. KOM(2010) 2020 endg. vom 3. März 2010.
[3] Mitteilung der Kommission „Den Binnenmarkt weiter ausbauen: mehr Chancen für die Menschen und die Unternehmen“. COM(2015) 550 final vom 28. Oktober 2015.
[4] Mitteilung über eine Strategie für einen digitalen Binnenmarkt für Europa. COM(2015) 192 final vom 6. Mai 2015.
[5] COM(2016) 176 final vom 19. April 2016.
[6] KOM(2011) 311 endg. vom 1. Juni 2011.

(6) Über die Festlegung der IKT-Spezifikationen sollte nach Konsultation der Europäischen Multi-Stakeholder-Plattform für die IKT-Normung entschieden werden, die von der Kommission mit dem Beschluss 2011/C 349/04 ([1]) eingerichtet wurde, ergänzt durch weitere Formen der Konsultation sektoraler Sachverständiger.

(7) Die Europäische Multi-Stakeholder-Plattform für die IKT-Normung bewertete, ob auf die nachfolgend aufgeführten technischen Spezifikationen bei der Vergabe öffentlicher Aufträge Bezug genommen werden kann, und gab diesbezüglich eine positive Stellungnahme ab: „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) und „DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security“ (DANE-SMTP), entwickelt von der Internet Engineering Task Force (IETF), sowie „Structured Threat Information Expression“ (STIX 1.2) und „Trusted Automated Exchange of Indicator Information“ (TAXII 1.1), entwickelt von der Organization for the Advancement of Structured Information Standards (OASIS). Die Bewertung und die Ratschläge der Plattform wurden anschließend sektoralen Sachverständigen zur Konsultation vorgelegt, die ebenfalls eine positive Stellungnahme hinsichtlich der Festlegung abgaben.

(8) Die technische Spezifikation „SPF“, die von IETF entwickelt wurde, ist eine offene Norm, mit der eine technische Methode zur Erkennung einer Fälschung der Absenderadresse spezifiziert wird. SPF bietet die Möglichkeit, zu überprüfen, ob eine Nachricht von einem dafür autorisierten Server verschickt wird. Es handelt sich um ein einfaches System zur Validierung von E-Mails, das darauf ausgerichtet ist, E-Mail-Spoofing zu erkennen, indem es einen Mechanismus bereitstellt, über den der Empfänger eines E-Mail-Austauschs überprüfen kann, ob von einer Domain eingehende Nachrichten von einem von den Administratoren dieser Domain autorisierten Host stammen. Mithilfe von SPF sollen Spammer daran gehindert werden, Nachrichten mit gefälschten Absenderadressen („from-address“) einer bestimmten Domain zu versenden. Die Empfänger können anhand eines SPF-Eintrags feststellen, ob eine Nachricht, die vorgibt, von dieser Domain zu stammen, von einem autorisierten Mail-Server kommt.

(9) „STARTTLS-SMTP“ wurde von IETF entwickelt und bietet die Möglichkeit, eine bestehende unsichere Verbindung zu einer sicheren Verbindung aufzurüsten. STARTTLS ist eine Erweiterung des Simple Mail Transfer Protocol (SMTP), über das ein SMTP-Server und -Client für eine private, authentifizierte Kommunikation im Internet eine Sicherung durch Transport Layer Security (TLS) nutzen können. Insbesondere ungesicherte E-Mail-Kommunikation ist ein häufiger Angriffspunkt für das Eindringen in Regierungsnetze. Wenn ein Nutzer eine E-Mail versendet, wird diese vom Mailserver des E-Mail-Anbieters des Nutzers an den Mailserver des Empfängers übertragen. Die Verbindung zwischen diesen beiden Mailservern kann im Vorfeld mit TLS gesichert werden. STARTTLS bietet die Möglichkeit, eine unverschlüsselte Verbindung (also in reinem Textformat) zu einer verschlüsselten TLS-Verbindung aufzurüsten.

(10) „DANE-SMTP“ wurde von IETF entwickelt und ist eine Reihe von Protokollen zur Verbesserung der Internetsicherheit, die es ermöglicht, Schlüssel in das Domain-Namen-System (DNS) zu integrieren und über DNSSEC (DNS-Security) zu sichern. Bei der Herstellung einer sicheren Verbindung mit einem unbekannten Partner ist eine Online-Überprüfung der Authentizität des Senders und des Empfängers wünschenswert. Das kann mithilfe von Zertifikaten, die von Zertifizierungsdiensteanbietern (Certificate Authority, CA) innerhalb des PKI-Systems ausgestellt wurden, oder mithilfe selbstsignierter Zertifikate erfolgen. Mit DANE kann der Inhaber einer Domain (Registrant) in einem DNSSEC-gesicherten DNS-Eintrag über die Online-Zertifikate hinaus weitere Informationen bereitstellen. Daher ist DANE für die aktive Bekämpfung von Angreifern besonders wichtig.

(11) „STIX 1.2“ wurde von OASIS entwickelt und ist eine Sprache, mit der Informationen über Cyberbedrohungen auf standardisierte und strukturierte Weise beschrieben werden können. Sie umfasst die wichtigsten Themen im Zusammenhang mit Daten über Cyberbedrohungen und erleichtert die Auswertung und den Austausch über Angriffe. Sie beschreibt ein umfassendes Paket von Informationen über Cyberbedrohungen, einschließlich Anzeichen für feindliche Aktivitäten, wie IP-Adressen und Hashwerte der Dateien sowie Kontextinformationen über Bedrohungen, beispielsweise feindliche Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures — TTPs), Angriffsziele sowie Campaigns and Courses of Action (COA). Die Gesamtheit dieser Informationen beschreibt die Motivation, Fähigkeiten und Aktivitäten des Cybergegners und trägt somit zur Abwehr solcher Angriffe bei.

(12) Mit der ebenfalls von OASIS entwickelten technischen Spezifikation „TAXII v1.1“ wird der vertrauenswürdige automatisierte Austausch von Informationen über Cyberbedrohungen standardisiert. TAXII definiert die Dienste und den Nachrichtenaustausch für das Teilen handlungsweisender Informationen über Cyberbedrohungen für die Erkennung, Vorbeugung und Eindämmung von Cyberangriffen über organisations-, produkt- oder dienstbezogene Grenzen hinweg. Mit TAXII können Organisationen das Lagebewusstsein für neue Bedrohungen verbessern und leicht Informationen mit Partnern teilen und dabei auf bestehenden Beziehungen und Systemen aufbauen —

([1]) Beschluss 2011/C 349/04 der Kommission vom 28. November 2011 zur Einrichtung einer Europäischen Multi-Stakeholder-Plattform für die IKT-Normung (ABl. C 349 vom 30.11.2011, S. 4).

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Auf die im Anhang aufgeführten technischen Spezifikationen kann bei der Vergabe öffentlicher Aufträge Bezug genommen werden.

Artikel 2

Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Brüssel, den 11. Dezember 2017

Für die Kommission
Der Präsident
Jean-Claude JUNCKER

ANHANG

Internet Engineering Task Force (IETF)

Nr.	Titel der technischen Spezifikation im IKT-Bereich
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.	Titel der technischen Spezifikation im IKT-Bereich
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information