COMMISSION IMPLEMENTING DECISION (EU) 2017/2288

of 11 December 2017

on the identification of ICT Technical Specifications for referencing in public procurement

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council ([1]), and in particular Article 13(1) thereof,

After consulting the European multi-stakeholder platform on ICT standardisation and sectoral experts

Whereas:

(1) Standardisation plays an important role in supporting the Europe 2020 strategy ([2]). Several flagship initiatives of the Europe 2020 strategy underlined the importance of voluntary standardisation in product or services markets to assure the compatibility and interoperability between products and services, foster technological development and support innovation.

(2) Standards are essential for European competitiveness and crucial for innovation and progress. The Commission Communications on the Single Market ([3]) and the Digital Single market ([4]) confirm the relevance of common standards to ensure the necessary interoperability of networks and systems in the European Digital Economy. This is reinforced with the adoption of the Communication on ICT Standardisation Priorities ([5]) where the Commission identifies priority ICT technologies where standardisation is considered critical to the completion of the Digital Single Market.

(3) The Communication from the Commission entitled 'A strategic vision for European standards: moving forward to enhance and accelerate the sustainable growth of the European economy by 2020' ([6]) recognised the specificity of standardisation in the field of information and communication technologies ('ICT'), where solutions, applications and services are often developed by global ICT Fora and Consortia that are today leading ICT standards development organisations.

(4) Regulation (EU) No 1025/2012 on European standardisation established a system whereby the Commission may decide to identify the most relevant and most widely accepted ICT technical specifications issued by organisations that are not European, international or national standardisation organisations, that might then be referenced, primarily to enable interoperability in public procurement. The possibility of using the full range of ICT technical specifications when procuring hardware, software and information technology services will enable interoperability between devices, services and applications, will help public administrations to avoid lock-in that occurs when the public procurer cannot change a provider after the expiration of the procurement contract because using ICT proprietary solutions, and it will encourage competition in the supply of interoperable ICT solutions.

(5) For the ICT technical specifications to be eligible for referencing in public procurement they must comply with the requirements set out in Annex II to Regulation (EU) No 1025/2012. Compliance with those requirements guarantees the public authorities that the ICT technical specifications are established in accordance with the principles of openness, transparency, impartiality and consensus that are recognised by the World Trade Organisation in the field of standardisation.

([1]) OJ L 316, 14.11.2012, p. 12.
([2]) Communication from the Commission entitled 'Europe 2020: A strategy for smart, sustainable and inclusive growth'. COM(2010) 2020 final of 3 March 2010.
([3]) Communication from the Commission 'upgrading the single market: more opportunities for people and business'. COM(2015) 550 final of 28 October 2015.
([4]) Communication on a Digital Single Market Strategy for Europe. COM(2015) 192 final of 6 May 2015.
([5]) COM(2016) 176 final of 19 April 2016.
([6]) COM(2011) 311 final of 1 June 2011.

(6) The decision to identify the ICT specification is to be adopted after consultation of the European multi-stakeholder platform on ICT standardisation set up by Commission Decision 2011/C 349/04 ([1]) complemented by other forms of consultation of sectoral experts.

(7) The European multi-stakeholder platform on ICT standardisation evaluated and gave a positive advice to the identification of the following technical specifications for referencing in public procurement: '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') and 'DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security' ('DANE-SMTP') developed by Internet Engineering Task Force (IETF); 'Structured Threat Information Expression' ('STIX 1.2') and 'Trusted Automated Exchange of Indicator Information' ('TAXII 1.1') developed by the Organization for the Advancement of Structured Information Standards ('OASIS'). The evaluation and advice of the platform was subsequently submitted to consultation of sectoral experts who confirmed the positive advice to its identification.

(8) 'SPF' technical specification developed by IETF is an open standard that specifies a technical method to detect sender address falsification. SPF offers the option of checking whether a message is sent from a server that is authorised to do so. It is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorised by that domain's administrators. The purpose of SPF is to prevent spammers from sending messages with forged 'From-addresses' at a particular domain. Recipients can refer to an SPF record to determine whether a message purporting to be from that domain comes from an authorised mail server.

(9) 'STARTTLS-SMTP' developed by IETF, is a way to take an existing insecure connection and upgrade it to a secure connection. STARTTLS is an extension to the Simple Mail Transfer Protocol ('SMTP') service that allows an SMTP server and client to use Transport Layer Security ('TLS') to provide private, authenticated communication over the Internet. Particularly unsecured e-mail communication supplies a major attack vector for breaching government networks. If a user sends an e-mail, the mail server of the user's mail provider will send this e-mail to the mail server of the receiver. The connection between these mail servers can be secured in advance with TLS. STARTTLS offers a way to upgrade an unencrypted (plain-text) connection to an encrypted TLS-connection.

(10) 'DANE-SMTP' developed by IETF is a suite of protocols to enhance Internet security by allowing keys to be placed into Domain Name System ('DNS') and secured by DNSSEC ('DNS Security'). When establishing a secure connection with an unknown party, an online check of the authenticity of the sending party and the destination is desirable. This can be done by certificates issued by certificate authorities ('CAs') within the PKI system, or by self-signed certificates. DANE allows the holder of a domain ('registrant') to provide additional information on top of the online certificates through a DNSSEC-secured DNS record. DANE is therefore particularly important for combating active attackers.

(11) 'STIX 1.2' developed by OASIS is a language for describing cyber threat information in a standardised and structured manner. It covers major topics when it comes to cyber threat data, facilitating the analysis and exchange about attacks. It characterises an extensive set of cyber threat information, including indicators of adversary activity such as IP addresses and file hashes and contextual information regarding threats such as adversary Tactics, Techniques and Procedures ('TTPs'); exploitation targets; Campaigns and Courses of Action ('COA'). Together this information completely characterises the cyber adversary's motivations, capabilities, and activities, and thus, help in defending against attacks.

(12) 'TAXII v1.1' technical specification also developed by OASIS standardises the trusted, automated exchange of cyber threat information. TAXII defines services and message exchanges for sharing actionable cyber threat information across organisation, product, or service boundaries in view of the detection, prevention, and mitigation of cyber threats. TAXII empowers organisations to achieve improved situational awareness about emerging threats and it enables organisations to easily share information with partners, while leveraging existing relationships and systems,

([1]) Commission Decision 2011/C 349/04 of 28 November 2011 setting up the European multi-stakeholder platform on ICT standardisation (OJ C 349, 30.11.2011, p. 4).

HAS ADOPTED THIS DECISION:

Article 1

The technical specifications listed in the Annex are eligible for referencing in public procurement.

Article 2

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 11 December 2017.

For the Commission
The President
Jean-Claude JUNCKER

ANNEX

Internet Engineering Task Force (IETF)

No	Title of ICT technical specification
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 for the Advancement of Structured Information Standards (OASIS)

No	Title of ICT technical specification
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information