DECISIONE DI ESECUZIONE (UE) 2017/2288 DELLA COMMISSIONE

dell'11 dicembre 2017

relativa all'individuazione delle specifiche tecniche delle TIC da utilizzare come riferimento negli appalti pubblici

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 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 del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio ([1]), in particolare l'articolo 13, paragrafo 1,

previa consultazione della piattaforma multilaterale europea delle parti interessate sulla normalizzazione delle TIC e degli esperti del settore,

considerando quanto segue:

(1) La normazione svolge un importante ruolo di sostegno alla strategia Europa 2020 ([2]). Diverse iniziative faro della strategia Europa 2020 hanno sottolineato l'importanza della normazione volontaria nei mercati dei prodotti o dei servizi al fine di garantire la compatibilità e l'interoperabilità tra prodotti e servizi, promuovere lo sviluppo tecnologico e sostenere l'innovazione.

(2) La presenza di norme è essenziale per la competitività europea e costituisce un elemento cruciale per l'innovazione e il progresso. Nelle sue comunicazioni sul mercato unico ([3]) e sul mercato unico digitale ([4]) la Commissione ha confermato l'importanza dell'esistenza di norme comuni per garantire la necessaria interoperabilità delle reti e dei sistemi nell'economia digitale europea. Tale posizione è stata rafforzata dall'adozione della comunicazione sulle priorità per la normazione delle TIC ([5]), nella quale la Commissione individua le tecnologie TIC prioritarie per le quali la normazione è considerata di importanza cruciale per il completamento del mercato unico digitale.

(3) La comunicazione della Commissione dal titolo «Una visione strategica per le norme europee: compiere passi avanti per favorire e accelerare la crescita sostenibile dell'economia europea entro il 2020» ([6]) riconosce la specificità della normazione nel settore delle tecnologie dell'informazione e della comunicazione (TIC), in cui soluzioni, applicazioni e servizi sono spesso sviluppati da forum e consorzi di TIC internazionali che si sono imposti come organismi leader nell'elaborazione delle norme TIC.

(4) Il regolamento (UE) n. 1025/2012 sulla normazione europea ha stabilito un sistema mediante il quale la Commissione può decidere di individuare le specifiche tecniche delle TIC più pertinenti e maggiormente accettate, elaborate da organizzazioni diverse dalle organizzazioni di normazione europee, internazionali o nazionali, cui è possibile fare riferimento in primo luogo per consentire l'interoperabilità in materia di appalti pubblici. La possibilità di utilizzare tutta la gamma di specifiche tecniche delle TIC in occasione dell'acquisto di hardware, software e servizi di tecnologia dell'informazione consentirà di realizzare l'interoperabilità tra dispositivi, servizi e applicazioni, contribuirà a evitare la dipendenza da un unico fornitore delle pubbliche amministrazioni, che si verifica quando il committente pubblico non può cambiare fornitore dopo la scadenza del contratto di appalto a causa dell'impiego di soluzioni proprietarie, e promuoverà un clima di concorrenza per l'offerta di soluzioni TIC interoperabili.

(5) Per essere ammissibili ai fini dell'utilizzo come riferimento negli appalti pubblici, le specifiche tecniche delle TIC devono rispettare le prescrizioni di cui all'allegato II del regolamento (UE) n. 1025/2012. La conformità a tali requisiti garantisce alle autorità pubbliche che le specifiche tecniche delle TIC siano stabilite nel rispetto dei principi di apertura, trasparenza, imparzialità e consenso riconosciuti dall'Organizzazione mondiale del commercio nel campo della normazione.

([1]) GU L 316 del 14.11.2012, pag. 12.
([2]) Comunicazione della Commissione «Europa 2020: Una strategia per una crescita intelligente, sostenibile e inclusiva». COM(2010) 2020 definitivo del 3.3.2010.
([3]) Comunicazione della Commissione «Migliorare il mercato unico: maggiori opportunità per i cittadini e per le imprese». COM(2015) 550 final del 28 ottobre 2015.
([4]) Comunicazione sulla strategia per il mercato unico digitale in Europa. COM(2015) 192 final del 6 maggio 2015.
([5]) COM(2016) 176 final del 19 aprile 2016.
([6]) COM (2011) 311 def. del 1º giugno 2011.

(6) La decisione di individuare le specifiche delle TIC va adottata previa consultazione della piattaforma multilaterale europea delle parti interessate sulla normalizzazione delle TIC, istituita dalla decisione 2011/C 349/04 della Commissione ([1]), integrata da altre forme di consultazione di esperti del settore.

(7) La piattaforma multilaterale europea delle parti interessate sulla normalizzazione delle TIC ha valutato e ha espresso un parere positivo sull'individuazione delle seguenti specifiche tecniche ai fini dell'utilizzo come riferimento negli appalti pubblici: «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), elaborate dall'Internet Engineering Task Force (IETF), nonché «Structured Threat Information Expression» (STIX 1.2) e «Trusted Automated Exchange of Indicator Information» (TAXII 1.1) elaborate dall'Organizzazione per la promozione delle norme sulle informazioni strutturate (OASIS). La valutazione e il parere della piattaforma sono stati successivamente sottoposti per consultazione a esperti del settore che hanno confermato il parere positivo sull'individuazione delle specifiche.

(8) La specifica tecnica SPF sviluppata dall'IETF è una norma aperta che specifica un metodo tecnico per rilevare contraffazioni dell'indirizzo del mittente. Il sistema SPF offre la possibilità di controllare se un messaggio sia inviato da un server autorizzato a farlo. Si tratta di un sistema semplice di convalida dell'indirizzo di posta elettronica, progettato per rilevare lo spoofing di indirizzi tramite un meccanismo che permette ai destinatari di controllare se il messaggio in arrivo da un determinato dominio sia stato inviato da un host autorizzato dall'amministratore di tale dominio. Lo scopo del sistema SPF è impedire agli spammer di inviare messaggi da mittenti contraffatti di un determinato dominio. I destinatari possono fare riferimento a un record SPF per stabilire se un messaggio che sembra arrivare da un determinato dominio sia stato effettivamente inviato da un server di posta elettronica autorizzato.

(9) STARTTLS-SMTP, sviluppato dall'IETF, è un metodo per rendere sicura una connessione non sicura. STARTTLS è un'estensione del servizio Simple Mail Transfer Protocol (SMTP) che permette ai server e ai client SMTP di usare il protocollo Transport Layer Security (TLS) per fruire di una comunicazione privata autenticata via Internet. In particolare la comunicazione tramite posta elettronica non sicura rappresenta uno dei principali vettori di attacco per infiltrarsi in una rete governativa. Quando un utente invia un messaggio di posta elettronica, il server di posta del fornitore del servizio di posta elettronica lo invia al server di posta del destinatario. La connessione tra questi server di posta può essere resa sicura prima dell'invio tramite il protocollo TLS. STARTTLS offre un modo per trasformare una connessione non criptata (solo testo) in una connessione TLS criptata.

(10) DANE-SMTP, sviluppato dall'IETF, è una serie di protocolli atti a migliorare la sicurezza di Internet permettendo di inserire chiavi crittografiche nel Domain Name System (DNS) e di renderle sicure tramite DNSSEC (DNS security). Quando si crea un collegamento sicuro con un corrispondente sconosciuto è auspicabile un controllo online dell'autenticità del mittente e del destinatario. A questo scopo è possibile utilizzare certificati emessi da un'autorità di certificazione (CA) nell'infrastruttura a chiave pubblica (PKI), oppure certificati autofirmati. DANE permette all'intestatario di un dominio (registrante) di fornire informazioni supplementari in aggiunta ai certificati online mediante un record DNS reso sicuro tramite DNSSEC. Per questo DANE è particolarmente importante per contrastare gli attacchi attivi.

(11) STIX 1.2, sviluppato da OASIS, è un linguaggio per redigere informazioni relative a minacce informatiche in modo standardizzato e strutturato. Esso contempla le principali tipologie di dati relativi alle minacce informatiche, facilitando l'analisi degli attacchi e lo scambio in merito. Il linguaggio caratterizza una vasta gamma di informazioni relative alle minacce informatiche, compresi gli indicatori di attività avversarie, come gli indirizzi IP, gli hash dei file e le informazioni contestuali relative alle minacce, come tattiche, tecniche e procedure avversarie (TTP); obiettivi di sfruttamento; campagne e linee di condotta (COA). Nel loro insieme queste informazioni caratterizzano in modo completo le motivazioni, le capacità e le attività degli avversari informatici, dando quindi un contributo alla difesa dagli attacchi.

(12) La specifica tecnica TAXII v1.1, anch'essa sviluppata da OASIS, stabilisce una norma per lo scambio affidabile e automatizzato di informazioni relative alle minacce informatiche. TAXII definisce i servizi e lo scambio di messaggi finalizzati alla condivisione di informazioni relative a minacce informatiche oltre i confini di un'organizzazione, di un prodotto o di un servizio per individuare, prevenire e attenuare le minacce informatiche. TAXII mette le organizzazioni nella posizione di raggiungere un livello superiore di conoscenza situazionale riguardo alle minacce emergenti e permette loro di scambiare agevolmente informazioni con i partner facendo leva su relazioni e sistemi esistenti.

([1]) Decisione 2011/C 349/04 della Commissione, del 28 novembre 2011, che istituisce la piattaforma multilaterale europea delle parti interessate sulla normalizzazione delle tecnologie dell'informazione e della comunicazione (TIC) (GU C 349 del 30.11.2011, pag. 4).

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Le specifiche tecniche elencate nell'allegato sono ammissibili ai fini dell'utilizzo come riferimento negli appalti pubblici.

Articolo 2

La presente decisione entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, l'11 dicembre 2017

Per la Commissione
Il presidente
Jean-Claude JUNCKER

ALLEGATO

Internet Engineering Task Force (IETF)

n.	Titolo della specifica tecnica delle 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)

Organizzazione per la promozione delle norme sulle informazioni strutturate (OASIS)

n.	Titolo della specifica tecnica delle TIC
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information