DECYZJA WYKONAWCZA KOMISJI (UE) 2017/2288

z dnia 11 grudnia 2017 r.

w sprawie wskazania specyfikacji technicznych ICT na potrzeby dokonywania odniesień w zamówieniach publicznych

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE ([1]), w szczególności jego art. 13 ust. 1,

po konsultacji z ekspertami z europejskiej wielostronnej platformy ds. normalizacji ICT i z ekspertami branżowymi,

a także mając na uwadze, co następuje:

(1) Kwestie normalizacji odgrywają istotną rolę we wspieraniu realizacji strategii „Europa 2020" ([2]). W kilku inicjatywach przewodnich strategii „Europa 2020" podkreślono znaczenie dobrowolnej normalizacji na rynkach produktowych lub usługowych, przeprowadzanej w celu zapewnienia zgodności i interoperacyjności między produktami i usługami, pobudzania rozwoju technologicznego i wspierania innowacji.

(2) Normy są niezbędne dla konkurencyjności Europy i mają kluczowe znaczenie dla innowacyjności i postępu. W komunikacie Komisji w sprawie jednolitego rynku ([3]) i jednolitego rynku cyfrowego ([4]) potwierdzają znaczenie wspólnych norm niezbędnych do zapewnienia interoperacyjności sieci i systemów w europejskiej gospodarce cyfrowej. Przekaz ten został wzmocniony wraz z przyjęciem komunikatu dotyczącego priorytetów w normalizacji ICT ([5]), w którym Komisja określa najważniejsze technologie ICT, w przypadku których normalizacja jest uznawana za element o kluczowym znaczenie dla ukończenia tworzenia jednolitego rynku.

(3) W komunikacie Komisji zatytułowanym „Strategiczna wizja w zakresie norm europejskich – Postęp w celu poprawy i przyspieszenia zrównoważonego wzrostu gospodarki europejskiej do roku 2020" ([6]) uznano specyfikę normalizacji w dziedzinie technologii informacyjno-komunikacyjnych (ICT), w przypadku których rozwiązania, aplikacje i usługi są często opracowywane przez światowe fora i konsorcja ICT, które są obecnie czołowymi organizacjami w zakresie opracowywania norm w dziedzinie ICT.

(4) Rozporządzeniem (UE) nr 1025/2012 w sprawie normalizacji europejskiej ustanowiono system, zgodnie z którym Komisja może podjąć decyzję o wskazaniu najbardziej odpowiednich i najszerzej akceptowanych specyfikacji technicznych ICT wydanych przez organizacje, które nie są europejskimi, międzynarodowymi ani krajowymi organizacjami normalizacyjnymi, do których to norm można stosować odniesienia, głównie w celu zapewnienia interoperacyjności w zamówieniach publicznych. Możliwość korzystania z pełnego zakresu specyfikacji technicznych ICT przy zamawianiu sprzętu, oprogramowania i usług informatycznych ułatwi zapewnienie interoperacyjności urządzeń, usług i aplikacji oraz pomoże organom administracji publicznej uniknąć sytuacji, w których jednostka udzielająca zamówienia nie może zmienić dostawcy po upływie umowy dotyczącej tego zamówienia ze względu na wykorzystanie prawnie zastrzeżonych rozwiązań ICT; możliwość ta przyczyni się także do rozwoju konkurencji w zakresie dostarczania interoperacyjnych rozwiązań ICT.

(5) Aby specyfikacje techniczne ICT kwalifikowały się do celów dokonywania odniesień w zamówieniach publicznych, muszą one spełniać wymagania określone w załączniku II do rozporządzenia (UE) nr 1025/2012. Zgodność z tymi wymaganiami stanowi dla organów publicznych gwarancję, że specyfikacje techniczne ICT są ustalane zgodnie z zasadami przejrzystości, otwartości, przejrzystości, bezstronności i konsensusu uznawanymi przez Światową Organizację Handlu w dziedzinie normalizacji.

([1]) Dz.U. L 316 z 14.11.2012, s. 12.
([2]) Komunikat Komisji „Europa 2020 – Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu". COM(2010) 2020 final z dnia 3 marca 2010 r.
([3]) Komunikat Komisji „Usprawnianie jednolitego rynku: więcej możliwości dla obywateli i przedsiębiorstw". COM(2015) 550 final z dnia 28 października 2015 r.
([4]) Komunikat „Strategia jednolitego rynku cyfrowego dla Europy". COM(2015) 192 final z dnia 6 maja 2015 r.
([5]) COM(2016) 176 final z dnia 19 kwietnia 2016 r.
([6]) COM (2011) 311 final z dnia 1 czerwca 2011 r.

(6) Decyzję o wskazaniu specyfikacji ICT przyjmuje się po konsultacji z ekspertami z europejskiej wielostronnej platformy ds. normalizacji ICT, ustanowionej decyzją Komisji 2011/C 349/04 ([1]), oraz po dodatkowych konsultacjach z ekspertami branżowymi.

(7) Europejska wielostronna platforma ds. normalizacji ICT dokonała oceny i wydała pozytywną opinię odnośnie do wskazania następujących specyfikacji technicznych na potrzeby dokonywania odniesień w zamówieniach publicznych: „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«)" oraz „DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (»DANE-SMTP«)" opracowanych przez grupę zadaniową ds. inżynierii internetowej (IETF); „Structured Threat Information Expression (»STIX 1.2«)" oraz „Trusted Automated Exchange of Indicator Information (»TAXII 1.1«)" opracowanych przez Organizację na rzecz Promowania Standaryzacji Norm Transmisji Danych (OASIS). Ocenę i porady platformy przekazano następnie do konsultacji ekspertom branżowym, którzy również wydali pozytywną opinię w sprawie jej wskazań.

(8) Specyfikacja techniczna „SPF" opracowana przez IETF to otwarta specyfikacja techniczna, która określa techniczny sposób wykrywania fałszowania adresu nadawcy. SPF oferuje możliwość sprawdzenia, czy wiadomość została wysłana z upoważnionego do tego serwera. To prosty system weryfikacji wiadomości e-mail zaprojektowany w celu wykrywania spoofingu dzięki dostarczeniu mechanizmu umożliwiającego otrzymywanie rekordów wymiany poczty, aby sprawdzić, czy poczta przychodząca z danej domeny została wysłana przez hosta upoważnionego przez administratora tej domeny. Celem SPF jest przeciwdziałanie wysyłaniu niechcianej korespondencji przez spamerów ze sfałszowanych adresów w ramach danej domeny. Odbiorcy mogą odwołać się do zapisu SPF, aby sprawdzić, czy wiadomość pochodząca jakoby z określonej domeny została wysłana z upoważnionego serwera pocztowego.

(9) „STARTTLS-SMTP" opracowana przez IETF jest sposobem przyjęcia obecnego niepewnego połączenia i zmiany jego statusu na połączenie bezpieczne. STARTTLS jest rozszerzeniem usługi protokołu SMTP, który pozwala serwerowi i klientowi SMTP wykorzystywać TLS do przekazywania prywatnych, uwierzytelnionych komunikatów za pośrednictwem internetu. Zwłaszcza niezabezpieczona komunikacja elektroniczna stanowi poważny kanał umożliwiający włamanie do sieci rządowych. Gdy nadawca wysyła wiadomość pocztą elektroniczną, serwer pocztowy dostawcy usług poczty elektronicznej przesyła tę wiadomość do serwera pocztowego odbiorcy. Połączenie między tymi serwerami pocztowymi mogą być z wyprzedzeniem zabezpieczone za pomocą TLS. STARTTLS zapewnia sposób podniesienia statusu niezaszyfrowanych (plain-text) połączeń do zaszyfrowanych połączeń TLS.

(10) „DANE-SMTP" opracowane przez IETF to zbiór protokołów, mających na celu zwiększenie bezpieczeństwa internetu dzięki możliwości umiejscowienia kluczy w systemie nazw domen („DNS") oraz zabezpieczenia ich za pomocą DNSSEC („DNS Security"). Przy ustanawianiu bezpiecznego połączenia z nieznanym korespondentem pożądane jest sprawdzenie *online* autentyczności strony wysyłającej i jej miejsca działania. Można tego dokonać za pomocą zaświadczeń wydawanych przez organy certyfikujące („CA") w ramach systemu PKI lub za pomocą autonomicznych zaświadczeń. DANE umożliwia właścicielowi domeny („rejestrujący") dostarczanie dodatkowych informacji oprócz internetowych certyfikatów za pośrednictwem rekordów DNZ zabezpieczonych za pomocą DNSSEC. DANE ma zatem szczególne znaczenie dla zwalczania aktywnie działających internetowych agresorów.

(11) „STIX 1.2" opracowany przez OASIS jest językiem do opisu informacji o zagrożeniu cybernetycznym w sposób znormalizowany i usystematyzowany. Ujęto w nim główne kwestie w zakresie danych stanowiących zagrożenie cybernetyczne, co ułatwia analizę danych i wymianę informacji na temat ataków. Dostarcza on charakterystyki szerokiego zestawu danych stanowiących zagrożenie cybernetyczne, w tym wskaźników dotyczących wrogiej działalności, takich jak adresy IP i hasze plików oraz informacji kontekstowych dotyczących zagrożeń takich jak szkodliwe taktyki, techniki i procedury („TTP"); cele eksploatacyjne; kampanie i sposoby działania („COA"). Informacje te łącznie całkowicie charakteryzują motywacje cybernetycznego przeciwnika, jego potencjał i działania i w ten sposób pomagają obronić się przed atakami.

(12) Specyfikacja techniczna „TAXII v1.1", również opracowana przez OASIS normalizuje zaufaną, automatyczną wymianę informacji o zagrożeniu cybernetycznym. TAXII określa wymianę usług i wiadomości do celów wymiany użytecznych informacji o zagrożeniu cybernetycznym w obrębie organizacji, produktu lub usługi w celu wykrycia zagrożeń cybernetycznych, zapobieżenia im i złagodzenia ich skutków. TAXII zapewnia organizacjom możliwość uzyskania lepszej orientacji sytuacyjnej w zakresie pojawiających się zagrożeń i umożliwia organizacjom łatwą wymianę informacji z partnerami przy jednoczesnym wykorzystaniu istniejących powiązań i systemów,

([1]) Decyzja Komisji 2011/C 349/04 z dnia 28 listopada 2011 r. ustanawiająca europejską wielostronną platformę ds. normalizacji ICT (Dz.U. C 349 z 30.11.2011, s. 4).

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Specyfikacje techniczne wymienione w załączniku kwalifikują się na potrzeby dokonywania odniesień w zamówieniach publicznych.

Artykuł 2

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 11 grudnia 2017 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

ZAŁĄCZNIK

Grupa zadaniowa ds. inżynierii internetowej (IETF)

Nr	Tytuł specyfikacji technicznej ICT
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)

Organizacja na rzecz Promowania Standaryzacji Norm Transmisji Danych (OASIS)

Nr	Tytuł specyfikacji technicznej ICT
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information