KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2017/2288

av den 11 december 2017

om fastställande av tekniska specifikationer för informations- och kommunikationsteknik som hänvisning vid offentlig upphandling

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG ([1]), särskilt artikel 13.1,

efter samråd med Europeiska flerpartsforumet för IKT-standardisering och med experter inom sektorn, och

av följande skäl:

(1) Standardisering fyller en viktig funktion för att stödja Europa 2020-strategin ([2]). I flera flaggskeppsinitiativ i Europa 2020-strategin framhålls vikten av frivillig standardisering på produkt- och tjänstemarknaderna för att säkerställa kompatibilitet och interoperabilitet mellan produkter och tjänster, stimulera teknisk utveckling och stödja innovation.

(2) Standarder är viktiga för den europeiska konkurrenskraften och avgörande för innovation och framsteg. I kommissionens meddelanden om den inre marknaden ([3]) och den inre digitala marknaden ([4]) bekräftas vikten av gemensamma standarder för att säkerställa den interoperabilitet som krävs mellan nätverk och system i den europeiska digitala ekonomin. Detta förstärktes genom antagandet av meddelandet om prioriteringar för informations- och kommunikationsteknisk standardisering ([5]), där kommissionen identifierade prioriterad IKT-teknik för vilken standardisering anses vara av kritisk betydelse för färdigställandet av den inre digitala marknaden.

(3) I kommissionens meddelande *En strategisk vision för europeiska standarder: bättre och snabbare hållbar tillväxt i den europeiska ekonomin före 2020* ([6]) framhävdes standardiseringens särdrag inom informations- och kommunikationsteknik (nedan kallad *IKT*), eftersom lösningar, tillämpningar och tjänster på området ofta utvecklas av globala IKT-forum och IKT-konsortier som i dag är ledande standardiseringsorganisationer på IKT-området.

(4) I förordning (EU) nr 1025/2012 om europeisk standardisering fastställs ett system där kommissionen kan besluta om att fastställa de mest relevanta och allmänt vedertagna tekniska specifikationerna på IKT-området som utfärdats av andra organisationer än europeiska, internationella eller nationella standardiseringsorganisationer, vilka det sedan får hänvisas till inom offentlig upphandling, i första hand för att möjliggöra interoperabilitet. Möjligheten att använda hela skalan av tekniska specifikationer på IKT-området vid upphandling av maskinvara, programvara och it-tjänster kommer att förbättra interoperabiliteten mellan utrustning, tjänster och tillämpningar, hjälpa offentliga förvaltningar att undvika den inlåsning som uppstår när en offentlig upphandlare inte kan byta leverantör efter det att kontraktet löper ut, eftersom leverantörsspecifika IKT-lösningar användes, samt stimulera konkurrens i utbudet av interoperabla IKT-lösningar.

(5) För att tekniska specifikationer på IKT-området ska komma i fråga för hänvisningar vid offentlig upphandling måste de uppfylla kraven i bilaga II till förordning (EU) nr 1025/2012. Efterlevnaden av dessa krav innebär att myndigheterna garanteras att de tekniska specifikationerna på IKT-området fastställs enligt de principer för öppenhet, transparens, rättvisa, opartiskhet och enighet som erkänts av Världshandelsorganisationen (WTO) i fråga om standardisering.

([1]) EUT L 316, 14.11.2012, s. 12.
([2]) Meddelande från kommissionen: *Europa 2020: En strategi för smart och hållbar tillväxt för alla*. KOM(2010) 2020 slutlig, 3 mars 2010.
([3]) Meddelande från kommissionen: *Att förbättra den inre marknaden – bättre möjligheter för individer och företag*. COM(2015) 550 final, 28 oktober 2015.
([4]) Meddelande från kommissionen: *En strategi för en inre digital marknad i Europa*. COM(2015) 192 final, 6 maj 2015.
([5]) COM (2016) 176 final, 19 april 2016.
([6]) KOM(2011) 311 slutlig, 1 juni 2011.

(6) Beslutet att fastställa IKT-specifikationer ska antas efter samråd med Europeiska flerpartsforumet för IKT-standardisering, som inrättats genom kommissionens beslut 2011/C 349/04 ([1]) och kompletterats med andra former av samråd med experter inom sektorn.

(7) Europeiska flerpartsforumet för IKT-standardisering utvärderade följande tekniska specifikationer och tillstyrkte att de kunde användas som hänvisning vid offentlig upphandling: ”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) och ”DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security” (DANE- SMTP) som utvecklats av Internet Engineering Task Force (IETF), samt ”Structured Threat Information Expression” (STIX 1.2) och ”Trusted Automated Exchange of Indicator Information” (TAXII 1.1) som utvecklats av Organization for the Advancement of Structured Information Standards (OASIS). Forumets utvärdering och råd överlämnades därefter till samråd med sektorsexperter, vilka bekräftade forumets positiva bedömning.

(8) Den tekniska specifikationen SPF, som utvecklats av IETF, är en öppen standard som specificerar en teknisk metod för upptäckt av förfalskade avsändaradresser. Med SPF går det att kontrollera om ett meddelande skickas från en server som har behörighet att skicka det. Det är ett enkelt e-postverifieringssystem avsett att upptäcka e-postförfalskningar och har en mekanism med vars hjälp mottagande e-postutbytare kan kontrollera att inkommande e-post från en domän kommer från en värd som har auktoriserats av domänens administratörer. Syftet med SPF är att förhindra skräppostspridare att skicka meddelanden med en förfalskad avsändaradress på en viss domän. Mottagarna kan gå till ett SPF-register för att avgöra om ett meddelande som utger sig för att komma från den aktuella domänen kommer från en auktoriserad e-postserver.

(9) STARTTLS-SMTP, som utvecklats av IETF, är ett sätt att uppgradera en befintlig osäker anslutning till en säker anslutning. STARTTLS är ett tillägg till tjänsten Simple Mail Transfer Protocol (SMTP) som gör att en SMTP-server och en SMTP-klient kan använda Transport Layer Security (TLS) för privat, autentiserad kommunikation över internet. I synnerhet oskyddad e-postkommunikation är en viktig attackväg för intrång i myndighetsnätverk. Om en användare skickar ett e-postmeddelande skickas det av användarens e-postleverantörs e-postserver till mottagarens e-postserver. Anslutningen mellan dessa e-postservrar kan göras säker i förväg med TLS. Med hjälp av STARTTLS kan en okrypterad anslutning (klartext) uppgraderas till en krypterad TLS-anslutning.

(10) DANE-SMTP, som utvecklats av IETF, är en protokollsvit som förbättrar internetsäkerheten genom att tillåta att nycklar placeras i domännamnssystemet (DNS) och säkras med DNSSEC (DNS-säkerhet). När en säker anslutning upprättas till en okänd part bör en onlinekontroll av både avsändaren och målet göras. Detta kan ske genom certifikat som utfärdats av certifikatutfärdare i PKI-systemet, eller genom självsignerade certifikat. Med hjälp av DANE kan domäninnehavaren (registranten) ange ytterligare information utöver onlinecertifikaten genom en DNSSEC-säkrad DNS-post. DANE är därför särskilt viktigt i kampen mot aktiva angripare.

(11) STIX 1.2, som utvecklats av OASIS, är ett språk för att beskriva information om cyberhot på ett standardiserat och strukturerat sätt. Det omfattar viktiga ämnen när det gäller data om cyberhot och gör det lättare att analysera och utbyta information om attacker. Det beskriver en omfattande uppsättning information om cyberhot, däribland indikatorer på fientlig verksamhet, t.ex. ip-adresser och filhashvärden, samt sammanhangsberoende information om hot, t.ex. fientliga taktiker, tekniker och procedurer (TTP), utnyttjandemål samt kampanjer och händelseförlopp (COA). Tillsammans ger dessa uppgifter en komplett beskrivning av cybermotståndarens motiv, förmåga och aktiviteter, och kan därför hjälpa till med försvaret mot attacker.

(12) Den tekniska specifikationen TAXII v1.1, som också har utvecklats av OASIS, standardiserar betrott, automatiserat utbyte av information om cyberhot. TAXII definierar tjänster och meddelandeutbyten för delning av användbar information om cyberhot över organisations-, produkt- och tjänstegränserna med avseende på att upptäcka, förebygga och minska cyberhoten. TAXII kan göra organisationer mer situationsmedvetna om nya hot och hjälpa dem att enkelt utbyta information med samarbetspartner, samtidigt som de drar nytta av befintliga relationer och system.

([1]) Kommissionens beslut 2011/C 349/04 av den 28 november 2011 om inrättande av Europeiska flerpartsforumet för IKT-standardisering (EUT C 349, 30.11.2011, s. 4).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

De tekniska specifikationerna i bilagan godkänns som hänvisning vid offentlig upphandling.

Artikel 2

Detta beslut träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 11 december 2017.

På kommissionens vägnar
Jean-Claude JUNCKER
Ordförande

BILAGA

Internet Engineering Task Force (IETF)

Nr	Benämning på teknisk specifikation för IKT
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	Benämning på teknisk specifikation för IKT
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information