KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2017/2288

af 11. december 2017

om udpegning af IKT-tekniske specifikationer, der kan henvises til i forbindelse med offentlige udbud

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF ([1]), særlig artikel 13, stk. 1,

efter høring af Den Europæiske Multistakeholderplatform for IKT-standardisering og af sektorspecifikke eksperter, og

ud fra følgende betragtninger:

(1) Standardisering spiller en vigtig rolle i Europa 2020-strategien ([2]). Flere flagskibsinitiativer i Europa 2020-strategien understreger betydningen af frivillig standardisering på produkt- eller tjenestemarkeder for at sikre kompatibilitet og interoperabilitet mellem produkter og tjenester, fremme teknologisk udvikling og støtte innovation.

(2) Standarder er afgørende for europæisk konkurrenceevne samt for innovation og fremskridt. Kommissionens meddelelser om henholdsvis det indre marked ([3]) og det digitale indre marked ([4]) bekræfter relevansen af fælles standarder med henblik på at sikre den nødvendige interoperabilitet mellem netværk og systemer i den europæiske digitale økonomi. Dette styrkes med vedtagelsen af meddelelsen om IKT-standardiseringsprioriteter ([5]), hvor Kommissionen indkredser prioriterede IKT-teknologier, hvor standardisering er afgørende for gennemførelsen af det digitale indre marked.

(3) I sin meddelelse »En strategisk vision for europæiske standarder: En indsats for at forbedre og fremskynde bæredygtig vækst i den europæiske økonomi inden 2020« ([6]) anerkender Kommissionen standardisering af informations- og kommunikationsteknologi (IKT) som et særligt felt, hvor løsninger, applikationer og tjenester ofte udvikles af globale IKT-fora og -konsortier, der er blevet førende inden for udviklingen af IKT-standarder.

(4) Ved forordning (EU) nr. 1025/2012 om europæisk standardisering indførtes en ordning, hvorved Kommissionen kan beslutte at udpege de mest relevante og mest anerkendte tekniske IKT-specifikationer udstedt af organisationer, der ikke er europæiske, internationale eller nationale standardiseringsorganisationer, og som der kan henvises til primært for at muliggøre interoperabilitet i forbindelse med offentlige udbud. Muligheden for at anvende det fulde spektrum af IKT-tekniske specifikationer ved indkøb af hardware, software og informationsteknologiske tjenesteydelser vil muliggøre interoperabilitet mellem udstyr, tjenesteydelser og applikationer, hjælpe den offentlige forvaltning til at undgå den fastlåsning, der opstår, når den offentlige indkøber på grund af proprietære IKT-løsninger ikke kan skifte udbyder efter udløbet af den offentlige kontrakt, og skabe konkurrence i udbuddet af interoperable IKT-løsninger.

(5) De IKT-tekniske specifikationer, der kan henvises til i forbindelse med offentlige udbud, skal være i overensstemmelse med kravene i bilag II til forordning (EU) nr. 1025/2012. Overholdelsen af disse krav er for de offentlige myndigheder en sikkerhed for, at de IKT-tekniske specifikationer er etableret i overensstemmelse med principperne om åbenhed, gennemsigtighed, upartiskhed og konsensus, som anerkendes af Verdenshandelsorganisationen (WTO) inden for standardisering.

([1]) EUT L 316 af 14.11.2012, s. 12.
([2]) Meddelelse fra Kommissionen, »EUROPA 2020, En strategi for intelligent, bæredygtig og inklusiv vækst«. KOM(2010) 2020 endelig af 3.3.2010.
([3]) Meddelelse fra Kommissionen, »Opgradering af det indre marked: flere muligheder for borgerne og virksomhederne«. COM (2015) 550 final af 28.10.2015.
([4]) Meddelelsen »Strategi for et digitalt indre marked i EU« COM(2015) 192 final af 6.5.2015.
([5]) KOM(2016) 176 final af 19.4.2016.
([6]) KOM (2011) 311 endelig af 1.6.2011.

(6) Afgørelsen om udpegning af bestemte IKT-specifikationer skal vedtages efter høring af Den Europæiske Multistakeholderplatform for IKT-standardisering, der er oprettet ved Kommissionens afgørelse 2011/C 349/04 ([1]), og vil blive suppleret af andre former for høring af sektorspecifikke eksperter.

(7) Den Europæiske Multistakeholderplatform for IKT-standardisering har evalueret og afgivet positiv udtalelse om udpegning af følgende tekniske specifikationer, der kan henvises til i forbindelse med offentlige udbud: »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«) og »DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (»DANE- SMTP«)«, der er udviklet af Internet Engineering Task Force (IETF) »Structured Threat Information Expression (»STIX 1.2«)« og »Trusted Automated Exchange of Indicator Information (»TAXII 1.1«)«, som er udviklet af Organization for the Advancement of Structured Information Standards (»OASIS«). Evalueringer og udtalelser om platformen blev efterfølgende forelagt sektorspecifikke eksperter til høring, og disse afgav også positiv udtalelse om udpegningen.

(8) Den tekniske specifikation »SPF«, der er udviklet af IETF, er en åben standard, der specificerer en teknisk metode til at påvise forfalskning af afsenderadresser. SPF giver mulighed for at kontrollere, om en meddelelse er sendt fra en server, der er bemyndiget hertil. Det drejer sig om et simpelt e-mail-valideringssystem, der er beregnet til at opdage e-mail-spoofing ved hjælp af en mekanisme, der gør det muligt at tillade modtagende mail-exchangere at kontrollere, at indkommende mail fra et domæne kommer fra en vært, der er godkendt af dette domænes administratorer. Formålet med SPF er at forhindre spammere i at sende meddelelser med forfalskede afsenderadresser i et bestemt domæne. Modtagerne kan slå op i en SPF-record for at fastslå, om en meddelelse, der foregiver at være fra det pågældende domæne, kommer fra en godkendt mailserver.

(9) »STARTTLS-SMTP«, der er udviklet af IETF, er en måde, hvorpå en eksisterende usikker forbindelse kan opgraderes til en sikker forbindelse. STARTTLS er en udvidelse af Simple Mail Transfer Protocol(»SMTP«)-tjenesten, der gør det muligt for en SMTP-server og en klient at anvende Transport Layer Security (»TLS«) til levering af privat, autentificeret kommunikation over internettet. Især usikret e-mail-kommunikation udgør en vigtig angrebsvej for indbrud i offentlige net. Når en bruger sender en e-mail, sender mailserveren hos brugerens mail-udbyder denne e-mail til modtagerens mailserver. Forbindelsen mellem disse mailservere kan sikres på forhånd med TLS. STARTTLS giver mulighed for at opgradere en ikke-krypteret (plain-text) forbindelse til en krypteret TLS-forbindelse.

(10) »DANE-SMTP«, der er udviklet af IETF, er en suite af protokoller, der forbedrer internetsikkerheden ved at gøre det muligt at anbringe nøgler i domænenavnesystemet (DNS), og at disse sikres ved hjælp af DNSSEC (»DNS-sikkerhed«). Ved oprettelsen af en sikker forbindelse med en ukendt part er det ønskeligt at gennemføre en online-kontrol af den afsendende parts autenticitet og af destinationen. Dette kan gøres ved hjælp af certifikater udstedt af certificeringsmyndigheder (»CA«) inden for PKI-systemet eller ved hjælp af self-signed-certifikater. DANE gør det muligt for indehaveren af et domæne (»registranten«) at forelægge supplerende oplysninger ud over onlinecertifikaterne gennem en DNSSEC-sikret record. DANE er derfor særligt vigtig ved bekæmpelse af aktive angribere.

(11) »STIX 1.2«, som er udviklet af OASIS, er et sprog til beskrivelse af informationer om cybertrusler på en standardiseret og struktureret måde. Det dækker vigtige emner vedrørende cybertrusselsdata og letter analysen og udvekslingen af oplysninger om angreb. Det karakteriserer et omfattende sæt cybertrusselsinformationer, herunder indikatorer vedrørende fjendtlig aktivitet, såsom IP-adresser, filhasher og kontekstuelle oplysninger om trusler, herunder fjendtlig taktik, teknik og fremgangsmåde (»Tactics, Techniques and Procedures — TTP«), udnyttelsesmål, kampagner og initiativer (»Courses of Action — COA«). Disse informationer udgør en samlet karakteristik af cybermodstanderens bevæggrunde, kapaciteter og aktiviteter og vil dermed kunne være et redskab i forsvaret mod angreb.

(12) Den tekniske specifikation »TAXII v1.1«, som også er udviklet af OASIS, standardiserer tilliden til automatiseret udveksling af informationer om cybertrusler. TAXII definerer tjeneste- og meddelelsesudvekslinger til deling af brugbare informationer om cybertrusler på tværs af organisations-, produkt- eller tjenestegrænser med henblik på afsløring, forebyggelse og afbødning af cybertrusler. TAXII giver organisationer mulighed for at opnå bedre situationsbevidsthed om nye trusler, og det sætter organisationer i stand til let at udveksle information med partnere, samtidig med at eksisterende forbindelser og systemer optimeres —

([1]) Kommissionens afgørelse 2011/C 349/04 af 28. november 2011 om oprettelse af Den Europæiske Multistakeholderplatform for Ikt-standardisering (EUT C 349 af 30.11.2011, s. 4).

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Der kan henvises til de i bilaget oplistede tekniske specifikationer i forbindelse med offentlige udbud.

Artikel 2

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 11. december 2017.

På Kommissionens vegne
Jean-Claude JUNCKER
Formand

BILAG

Internet Engineering Task Force (IETF)

Nr.	Betegnelse for IKT-teknisk specifikation
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

Nr.	Betegnelse for IKT-teknisk specifikation
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information