KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2016/650

af 25. april 2016

om fastlæggelse af standarder for sikkerhedsvurdering af kvalificerede signatur- og seglgenereringssystemer, jf. artikel 30, stk. 3, og artikel 39, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

(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. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 30, stk. 3, og artikel 39, stk. 2, og

ud fra følgende betragtninger:

(1) I bilag II til forordning (EU) nr. 910/2014 fastsættes kravene til kvalificerede elektroniske signaturgenereringssystemer og kvalificerede elektroniske seglgenereringssystemer.

(2) Udarbejdelsen af de tekniske specifikationer, der er nødvendige for at fremstille og markedsføre produkter under hensyntagen til det aktuelle teknologiske stade, varetages af organisationer, der er kompetente på standardiseringsområdet.

(3) ISO/IEC (Den Internationale Standardiseringsorganisation/Den Internationale Elektrotekniske Kommission) fastsætter de generelle begreber og principper inden for it-sikkerhed og fastlægger den generelle vurderingsmodel, der skal anvendes som grundlag for evalueringen af it-produkters sikkerhedsegenskaber.

(4) Den Europæiske Standardiseringsorganisation (CEN) har, i henhold til Kommissionens standardiseringsmandat M/460, udviklet standarder til kvalificerede elektroniske signatur- og seglgenereringssystemer, hvor data fra elektronisk signaturgenerering eller elektronisk seglgenerering opbevares i et fuldt ud, men ikke nødvendigvis udelukkende brugerforvaltet miljø. Disse standarder anses for at være egnede til at vurdere overensstemmelsen af sådanne systemer med de relevante krav i bilag II til forordning (EU) nr. 910/2014.

(5) I bilag II til forordning (EU) nr. 910/2014 fastsættes det, at kun en kvalificeret tillidstjeneste kan forvalte elektroniske signaturgenereringsdata på vegne af en underskriver. Sikkerhedskravene og deres respektive certificeringsspecifikationer er forskellige, når underskriveren er i besiddelse af et fysisk tillidsprodukt, og når en kvalificeret tillidstjeneste drives på vegne af en underskriver. For at håndtere begge situationer og begunstige udviklingen over tid af tillidsprodukter og vurderingsstandarder, der er egnede til specifikke behov, bør bilaget til denne afgørelse indeholde en liste over standarder, der omfatter begge situationer.

(6) På tidspunktet for vedtagelsen af Kommissionens afgørelse tilbød adskillige tillidstjenesteudbydere allerede løsninger til forvaltning af elektroniske signaturgenereringsdata på vegne af deres kunder. Certificering af produkter er på nuværende tidspunkt begrænset til hardwaresikkerhedsmoduler, der er certificeret efter andre standarder, men som endnu ikke er certificeret specifikt efter kravene til kvalificerede signatur- og seglgenereringssystemer. Imidlertid finder der endnu ikke offentliggjorte standarder, som f.eks. EN 419 211 (der finder anvendelse på elektroniske signaturer, der er genereret i et fuldt ud, men ikke nødvendigvis udelukkende brugerforvaltet miljø), til et lige så vigtigt marked for certificerede produkter på afstand. Eftersom standarder, der måtte være egnede til disse formål, for indeværende er under udvikling, vil Kommissionen, når disse standarder er tilgængelige og betragtes som værende forenelige med kravene i bilag II til forordning (EU) nr. 910/2014, komplementere denne afgørelse med dem. Indtil der findes en liste over sådanne standarder, kan der anvendes en alternativ proces til at foretage overensstemmelsesvurderingen af disse produkter i henhold til betingelserne i artikel 30, stk. 3, litra b), i forordning (EU) nr. 910/2014.

(7) I bilaget findes en liste over standard EN 419 211, som består af forskellige dele (1-6), der vedrører forskellige situationer. EN 419 211 del 5 og 419 211 del 6 fastsætter supplerende krav til miljøer for kvalificerede

([1]) EUT L 257 af 28.8.2014, s. 73.

signaturgenereringssystemer, som f.eks. kommunikation med sikre applikationer til signaturgenerering. Produktproducenter kan frit anvende disse supplerende krav. I henhold til betragtning 56 i forordning (EU) nr. 910/2014 bør certificering efter artikel 30 og 39 i samme forordning være begrænset til at beskytte signaturgenereringsdata, og applikationer til generering af signaturer er ikke omfattet af certificeringspligten.

(8) For at sikre at elektroniske signaturer eller segl, der er genereret af et kvalificeret signatur- eller seglgenereringssystem, på pålidelig vis er beskyttet mod forfalskning, jf. bilag II til forordning (EU) nr. 910/2014, er egnede kryptografiske algoritmer, nøglelængder og hashfunktioner en forudsætning for det certificerede produkts sikkerhed. Eftersom dette område ikke er blevet harmoniseret på europæiske niveau, bør medlemsstaterne arbejde sammen om at nå til enighed om, hvilke kryptografiske algoritmer, nøglelængder og hashfunktioner der skal finde anvendelse for elektroniske signaturer og segl.

(9) Ved vedtagelsen af denne afgørelse bliver Kommissionens beslutning 2003/511/EF [1] forældet. Den bør derfor ophæves.

(10) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er omhandlet i artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

1. De standarder for sikkerhedsvurdering af informationsteknologiprodukter, der finder anvendelse på certificeringen af kvalificerede elektroniske signaturgenereringssystemer eller kvalificerede elektroniske seglgenereringssystemer i henhold til artikel 30, stk. 3, litra a) eller artikel 39, stk. 2, i forordning (EU) nr. 910/2014, hvis de elektroniske signaturgenereringsdata eller elektroniske seglgenereringsdata opbevares i et fuldt ud, men ikke nødvendigvis udelukkende brugerforvaltet miljø, findes i en liste i bilaget til denne afgørelse.

2. Indtil Kommissionen udarbejder en liste over standarder for sikkerhedsvurdering af informationsteknologiprodukter, der finder anvendelse på certificeringen af kvalificerede elektroniske signaturgenereringssystemer eller kvalificerede elektroniske seglgenereringssystemer, hvor en kvalificeret tillidstjenesteudbyder forvalter de elektroniske signaturgenereringsdata eller elektroniske seglgenereringsdata på vegne af en underskriver eller på vegne af en forseglende part, er certificeringen af disse produkter baseret på en proces, som i henhold til artikel 30, stk. 3, litra b), anvender sikkerhedsniveauer, der er sammenlignelige med dem, der fremgår af artikel 30, stk. 3, litra a), og som anmeldes til Kommissionen af det offentlige eller private organ, der henvises til i artikel 30, stk. 1, i forordning (EU) nr. 910/2014.

Artikel 2

Beslutning 2003/511/EF ophæves.

Artikel 3

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

Udfærdiget i Bruxelles, den 25. april 2016.

På Kommissionens vegne
Jean-Claude JUNCKER
Formand

[1] Kommissionens beslutning 2003/511/EF af 14. juli 2003 om offentliggørelse af referencenumre på almindeligt anerkendte standarder for elektroniske signaturprodukter i overensstemmelse med Europa-Parlamentets og Rådets direktiv 1999/93/EF (EUT L 175 af 15.7.2003, s. 45).

BILAG

LISTE OVER SANDARDER SOM OMHANDLET I ARTIKEL 1, STK. 1

— ISO/IEC 15408 — Informationsteknologi — Sikkerhedsteknikker — Vurderingskriterier for IT-sikkerhed, del 1 til 3 som angivet nedenfor:

  — ISO/IEC 15408-1:2009 — Informationsteknologi — Sikkerhedsteknikker — Vurderingskriterier for IT-sikkerhed — Del 1. ISO, 2009.

  — ISO/IEC 15408-2:2008 — Informationsteknologi — Sikkerhedsteknikker — Vurderingskriterier for IT-sikkerhed — Del 2. ISO, 2008.

  — ISO/IEC 15408-3:2008 — Informationsteknologi — Sikkerhedsteknikker — Vurderingskriterier for IT-sikkerhed — Del 3. ISO, 2008.

  og

— ISO/IEC 18045:2008: Informationsteknologi — Sikkerhedsteknikker — Metodik til evaluering af it-sikkerhed

  og

— EN 419 211 — Beskyttelsesprofiler til enheder til generering af sikker signatur, del 1 til 6 — alt efter hvad der er relevant — som angivet nedenfor:

  — EN 419211-1:2014 — Protection profiles for secure signature creation device — Part 1 (EN 419211-1:2014 — Beskyttelsesprofiler til enheder til generering af sikker signatur — Del 1): Overview (Oversigt)

  — EN 419211-2:2013 — Beskyttelsesprofiler til enheder til generering af sikker signatur — Del 2: Udstyr med nøglegenerering

  — EN 419211-3:2013 — Beskyttelsesprofiler til enheder til generering af sikker signatur — Del 3: Enheder med nøgleimport

  — EN 419211-4:2013 — Beskyttelsesprofiler til enheder til generering af sikker signatur — Del 4: Udvidelse for enheder med nøglegenerering og pålidelig kanal til certifikatgenereringsapplikation

  — EN 419211-5:2013 — Beskyttelsesprofiler til enheder til generering af sikker signatur — Del 5: Udvidelse for enheder med nøglegenerering og pålidelig kanal til signaturgenereringsapplikation

  — EN 419211-6:2014 — Beskyttelsesprofiler til enheder til generering af sikker signatur — Del 6: Udvidelse til enheder med nøgleimport og pålidelig kanal til signaturgenereringsapplikation