COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

KOMMISJONENS GJENNOMFØRINGSBESLUTNING (EU) 2016/650

av 25. april 2016

om fastsettelse av standarder for sikkerhetsvurdering av kvalifiserte signatur- og seglframstillingssystemer i henhold til artikkel 30 nr. 3 og artikkel 39 nr. 2 i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked

EUROPAKOMMISJONEN HAR —

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF([1]), og særlig artikkel 30 nr. 3 og artikkel 39 nr. 2, og

ut fra følgende betraktninger:

1) I vedlegg II til forordning (EU) nr. 910/2014 fastsettes kravene til kvalifiserte elektroniske signaturframstillingssystemer og kvalifiserte elektroniske seglframstillingssystemer.

2) Oppgaven med å utarbeide de tekniske spesifikasjoner som er nødvendige for produksjon og omsetning av produkter, under hensyn til dagens teknologi, utføres av standardiseringsorganisasjoner.

3) ISO/IEC (Den internasjonale standardiseringsorganisasjon/Den internasjonale elektrotekniske standardiseringsorganisasjon) fastsetter de generelle begrepene og prinsippene for IT-sikkerhet og angir den generelle vurderingsmodellen som skal benyttes som grunnlag for vurdering av IT-produktenes sikkerhetsegenskaper.

4) Den europeiske standardiseringsorganisasjon (CEN) har i henhold til Kommisjonens standardiseringsmandat M/460 utarbeidet standarder for kvalifiserte elektroniske signatur- og seglframstillingssystemer, der elektroniske signaturframstillingsdata eller elektroniske seglframstillingsdata er holdt i et miljø som helt og holdent, men ikke nødvendigvis utelukkende, er brukerstyrt. Disse standardene anses som egnet til å vurdere om slike systemer samsvarer med de relevante kravene i vedlegg II til forordning (EU) nr. 910/2014.

5) I vedlegg II til forordning (EU) nr. 910/2014 er det fastsatt at bare en kvalifisert tilbyder av tillitstjenester kan håndtere elektroniske signaturframstillingsdata på vegne av en underskriver. Sikkerhetskravene og deres respektive sertifiseringsspesifikasjoner er forskjellige når underskriveren er i fysisk besittelse av et produkt, og når en kvalifisert tilbyder av tillitstjenester arbeider på vegne av underskriveren. For å håndtere begge situasjoner, og fremme utviklingen over tid av produkter og vurderingsstandarder som kan ivareta særlige behov, bør vedlegget til denne beslutning inneholde en liste over standarder som dekker begge situasjoner.

6) Når denne kommisjonsbeslutning vedtas, vil flere tilbydere av tillitstjenester allerede tilby løsninger for håndtering av elektroniske signaturframstillingsdata på vegne av sine kunder. Sertifisering av produkter er i dag begrenset til sikkerhetsmoduler i maskinvare som er sertifisert etter ulike standarder, men som ennå ikke er særskilt sertifisert etter kravene til kvalifiserte signatur- og seglframstillingssystemer. Offentliggjorte standarder, f.eks. EN 419 211 (som gjelder for elektroniske signaturer framstilt i et miljø som helt og holdent, men ikke nødvendigvis utelukkende, er brukerstyrt), finnes imidlertid ennå ikke for det like viktige markedet for sertifiserte fjernprodukter. Ettersom standarder som kan være hensiktsmessige for slike formål er under utvikling, vil Kommisjonen utfylle denne beslutning når de er tilgjengelige og anses å oppfylle kravene i vedlegg II til forordning (EU) nr. 910/2014. Inntil listen over slike standarder er opprettet, kan det benyttes en alternativ prosess til å foreta samsvarsvurderingen av slike produkter i henhold til vilkårene omhandlet i artikkel 30 nr. 3 bokstav b) i forordning (EU) nr. 910/2014.

7) Vedlegget inneholder en liste over EN 419 211, bestående av forskjellige deler (1–6) som dekker ulike situasjoner. EN 419 211 del 5 og 419 211 del 6 innebærer utvidede krav til miljøene for kvalifiserte signaturframstillingssystemer, for eksempel kommunikasjon med pålitelige signaturframstillingsprogrammer. Produktutviklere kan fritt anvende slike utvidede krav. I henhold til betraktning 56 i forordning (EU) nr. 910/2014 er sertifisering i henhold til artikkel 30 og 39 i nevnte forordning

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

begrenset til vern av signaturframstillingsdata, og signaturframstillingsprogrammer omfattes ikke av sertifiseringsplikten.

8) For å sikre at elektroniske signaturer og segl som genereres av et kvalifisert elektronisk signatur- eller seglframstillingssystem, er behørig beskyttet mot forfalskning som fastsatt i vedlegg II til forordning (EU) nr. 910/2014, er nøkkellengder og hash-funksjoner en forutsetning for det sertifiserte produktets sikkerhet. Ettersom dette ikke er blitt harmonisert på europeisk plan, bør medlemsstatene samarbeide for å enes om kryptografiske algoritmer, nøkkellengder og hash-funksjoner som skal benyttes i forbindelse med elektroniske signaturer og segl.

9) Ved vedtakelsen av denne beslutning blir kommisjonsvedtak 2003/511/EF([2]) foreldet. Det bør derfor oppheves.

10) Tiltakene fastsatt i denne beslutning er i samsvar med uttalelse fra komiteen nevnt i artikkel 48 i forordning (EU) nr. 910/2014 —

TRUFFET DENNE BESLUTNING:

Artikkel 1

1. De standarder for sikkerhetsvurdering av informasjonsteknologiprodukter som får anvendelse på sertifisering av kvalifiserte elektroniske signaturframstillingssystemer eller kvalifiserte elektroniske seglframstillingssystemer i samsvar med artikkel 30 nr. 3 bokstav a) eller artikkel 39 nr. 2 i forordning (EU) nr. 910/2014, der elektroniske signaturframstillingsdata eller elektroniske seglframstillingsdata er holdt i et miljø som helt og holdent, men ikke nødvendigvis utelukkende, er brukerstyrt, er oppført i vedlegget til denne beslutning.

2. Inntil Kommisjonen oppretter en liste over standarder for sikkerhetsvurdering av informasjonsteknologiprodukter som gjelder for sertifiseringen av kvalifiserte elektroniske signaturframstillingssystemer eller kvalifiserte elektroniske seglframstillingssystemer, skal – når en kvalifisert tilbyder av tillitstjenester håndterer elektroniske signaturframstillingsdata eller elektroniske seglframstillingsdata på vegne av en underskriver eller seglframstiller – sertifisering av slike produkter være basert på en prosess som i henhold til artikkel 30 nr. 3 bokstav b) benytter sikkerhetsnivåer som er sammenlignbare med dem som kreves i henhold til artikkel 30 nr. 3 bokstav a), og som er meldt til Kommisjonen av det offentlige eller private organet omhandlet i artikkel 30 nr. 1 i forordning (EU) nr. 910/2014.

Artikkel 2

Vedtak 2003/511/EF oppheves.

Artikkel 3

Denne beslutning trer i kraft den 20. dag etter at den er kunngjort i *Den europeiske unions tidende*.

Utferdiget i Brussel 25. april 2016.

For Kommisjonen

Jean-Claude JUNCKER

President

([2]) Kommisjonsvedtak 2003/511/EF av 14. juli 2003 om offentliggjøring av referansenumre for allment anerkjente standarder for elektroniske signaturprodukter i samsvar med europaparlaments- og rådsdirektiv 1999/93/EF (EUT L 175 av 15.7.2003, s. 45).

VEDLEGG

LISTE OVER STANDARDER NEVNT I ARTIKKEL 1 NR. 1

— ISO/IEC – 15408 – Information technology – Security techniques – Evaluation criteria for IT security, del 1–3 som oppført nedenfor:

  — ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – del 1. ISO, 2009.

  — ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – del 2. ISO, 2008.

  — ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – del 3. ISO, 2008.

  og

— ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation,

  og

— EN 419 211 – Protection profiles for secure signature creation device, del 1–6 – alt etter hva som er relevant – som oppført nedenfor:

  — EN 419211-1:2014 – — Protection profiles for secure signature creation device – del 1: Oversikt

  — EN 419211-2:2013 – — Protection profiles for secure signature creation device – del 2: System med nøkkelgenerering

  — EN 419211-3:2013 – — Protection profiles for secure signature creation device – del 3: System med nøkkelimport

  — EN 419211-4:2013 – — Protection profiles for secure signature creation device – del 4: Utvidelse for systemer med nøkkelgenerering og sikker kanal til applikasjon for sertifikatgenerering

  — EN 419211-5:2013 – — Protection profiles for secure signature creation device – del 5: Utvidelse for systemer med nøkkelgenerering og sikker kanal til applikasjon for signaturframstilling

  — EN 419211-6:2014 – — Protection profiles for secure signature creation device – del 6: Utvidelse for systemer med nøkkelimport og sikker kanal til applikasjon for signaturframstilling