KOMISJONI RAKENDUSOTSUS (EL) 2016/650,

25. aprill 2016,

millega kehtestatakse kvalifitseeritud allkirja andmise ja templi loomise vahendi turvalisuse hindamise standardid vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 30 lõikele 3 ja artikli 39 lõikele 2

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ, [1] eriti selle artikli 30 lõiget 3 ja artikli 39 lõiget 2,

ning arvestades järgmist:

(1) Määruse (EL) nr 910/2014 II lisas on sätestatud nõuded kvalifitseeritud e-allkirja andmise vahenditele ja kvalifitseeritud e-templi loomise vahenditele.

(2) Tehnoloogia praegust arengutaset arvestavate toodete valmistamiseks ja turuleviimiseks vajalike tehniliste kirjelduste koostamine on standardimise valdkonnas pädevate organisatsioonide ülesanne.

(3) ISO/IEC (Rahvusvaheline Standardiorganisatsioon / Rahvusvaheline Elektrotehnikakomisjon) kehtestab IT turvalisuse üldised mõisted ja põhimõtted ning määrab kindlaks IT-toodete turvaomaduste hindamisel aluseks võetava üldise mudeli.

(4) Euroopa Standardikomitee (CEN) on komisjoni antud standardimismandaadi M/460 alusel töötanud välja standardid kvalifitseeritud e-allkirja andmise ja e-templi loomise vahendite jaoks, mille puhul e-allkirja andmise ja e-templi loomise andmeid hoitakse täielikult, kuid mitte ilmtingimata ainuüksi kasutaja hallatavas keskkonnas. Neid standardeid peetakse sobivaiks, et hinnata selliste seadmete vastavust määruse (EL) nr 910/2014 II lisas sätestatud asjakohastele nõuetele.

(5) Määruse (EL) nr 910/2014 II lisas on sätestatud, et e-allkirja moodustamiseks vajalikke andmeid võib allkirja andja nimel hallata üksnes kvalifitseeritud usaldusteenuse osutaja. Turvalisusnõuded ja neile vastavad sertifitseerimistingimused on erinevad olenevalt sellest, kas toode on füüsiliselt allkirja andja valduses või tegutseb allkirja andja nimel kvalifitseeritud usaldusteenuse osutaja. Et mõlemat olukorda arvesse võtta ja soodustada aja jooksul konkreetsete vajadustega sobivate toodete ja hindamisstandardite arengut, loetletakse käesoleva otsuse lisas standardid, mis hõlmavad mõlemat olukorda.

(6) Komisjoni käesoleva otsuse vastuvõtmise ajal pakub mitu usaldusteenuse osutajat juba lahendusi e-allkirja moodustamiseks vajalike andmete haldamiseks nende klientide nimel. Praegu piirdub toodete sertifitseerimine füüsiliste turvamoodulitega, mida sertifitseeritakse küll eri standardite põhjal, kuid mida ei sertifitseerita veel konkreetselt kvalifitseeritud e-allkirja andmise ja e-templi loomise vahendite suhtes kehtivatest nõuetest lähtuvalt. Samas ei ole veel olemas standardi EN 419 211 (kohaldatakse e-allkirjade suhtes, mis luuakse täielikult, kuid mitte ilmtingimata ainuüksi kasutaja hallatavas keskkonnas) laadseid avaldatud standardeid, mis kehtiksid sama olulise sertifitseeritud kaugtoodete turu suhtes. Standardeid, mis võiksid selliseks otstarbeks sobida, koostatakse praegu; kui need valmis saavad ja leitakse, et nad vastavad määruse (EL) nr 910/2014 II lisas sätestatud nõuetele, täiendab komisjon käesolevat otsust. Kuni selliste standardite loetelu koostamiseni võib selliste toodete vastavust hinnata alternatiivsete protsesside kohaselt vastavalt määruse (EL) nr 910/2014 artikli 30 lõike 3 punktis b sätestatud tingimustele.

(7) Lisas on nimetatud standard EN 419 211, mis koosneb eri olukordi käsitlevatest eraldi osadest (osad 1–6). EN 419 211 osad 5 ja 6 käsitlevad laiendusi, mis on seotud kvalifitseeritud allkirja loomise vahendi keskkonnaga,

[1] ELT L 257, 28.8.2014, lk 73.

nt andmevahetus usaldatavate allkirja loomise rakendustega. Tootjatel on vabadus selliseid laiendusi rakendada. Vastavalt määruse (EL) nr 910/2014 põhjendusele 56 piirdub selle määruse artiklite 30 ja 39 kohane sertifitseerimine allkirja moodustamiseks kasutatavate andmete kaitsmisega ning allkirja andmise rakendused jäävad sertifitseerimise ulatusest välja.

(8) Tagamaks, et kvalifitseeritud e-allkirja andmise või e-templi loomise vahendiga loodavad e-allkirjad või e-templid on võltsimise vastu kindlalt kaitstud, nagu on nõutud määruse (EL) nr 910/2014 II lisas, tuleb sertifitseeritud toote turvalisuse eeltingimusena kasutada sobivaid krüptoalgoritme, võtmepikkusi ja räsifunktsioone. Neid küsimusi ei ole Euroopa tasandil ühtlustatud ning seega peaksid liikmesriigid tegema koostööd, et leppida kokku krüptoalgoritmides, võtmepikkustes ja räsifunktsioonides, mida tuleb e-allkirjade ja e-templite puhul kasutada.

(9) Käesoleva otsuse vastuvõtmisega minetab komisjoni otsus 2003/511/EÜ [1] asjakohasuse. Seepärast tuleks see kehtetuks tunnistada.

(10) Käesoleva otsusega ette nähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artiklis 48 nimetatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

1. Käesoleva otsuse lisas on loetletud infotehnoloogiatoodete turvalisuse hindamise standardid, mida kohaldatakse kvalifitseeritud e-allkirja andmise vahendite või kvalifitseeritud e-templi loomise vahendite sertifitseerimise suhtes vastavalt määruse (EL) nr 910/2014 artikli 30 lõike 3 punktile a või artikli 39 lõikele 2, kui e-allkirja moodustamiseks või e-templi loomiseks vajalikke andmeid hoitakse täielikult, kuid mitte ilmtingimata ainuüksi kasutaja hallatavas keskkonnas.

2. Kuni ajani, mil komisjon koostab loetelu infotehnoloogiatoodete turvalisuse hindamise standarditest, mida kohaldatakse kvalifitseeritud e-allkirja andmise vahendite või kvalifitseeritud e-templi loomise vahendite sertifitseerimise suhtes, kui allkirja andja või templi looja nimel haldab e-allkirja moodustamiseks või e-templi loomiseks vajalikke andmeid kvalifitseeritud usaldusteenuse osutaja, toimub selliste toodete sertifitseerimine protsessi kohaselt, mis vastavalt määruse (EL) nr 910/2014 artikli 30 lõike 3 punktile b kasutab artikli 30 lõike 3 punktis a nõutud turbeastmetega samaväärseid turbeastmeid ja millest artikli 30 lõikes 1 osutatud avalik-õiguslik või eraõiguslik asutus on komisjonile teatanud.

Artikkel 2

Otsus 2003/511/EÜ tunnistatakse kehtetuks.

Artikkel 3

Käesolev otsus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Brüssel, 25. aprill 2016

Komisjoni nimel

president

Jean-Claude JUNCKER

[1] Komisjoni 14. juuli 2003. aasta otsus 2003/511/EÜ, milles käsitletakse digitaalallkirjaga seotud toodete üldtunnustatud standardite viitenumbrite avaldamist kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga 1999/93/EÜ (ELT L 175, 15.7.2003, lk 45).

LISA

ARTIKLI 1 LÕIKES 1 OSUTATUD STANDARDITE LOETELU

— ISO/IEC 15408 – Information technology – Security techniques – Evaluation criteria for IT security, osad 1–3 järgmiselt:

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

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

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

  ning

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

  ning

— EN 419 211 – Protection profiles for secure signature creation device, osad 1–6 – vastavalt vajadusele – järgmiselt:

  — EN 419211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview

  — EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation

  — EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import

  — EN 419211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application

  — EN 419211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application

  — EN 419211-6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application