FRAMKVÆMDARÁKVÖRÐUN FRAMKVÆMDASTJÓRNARINNAR (ESB) 2016/650 **2019/EES/101/07**

frá 25. apríl 2016

um staðla fyrir öryggismat fullgilds undirskriftar- og innsiglisbúnaðar skv. 3. mgr. 30. gr. og 2. mgr. 39. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 910/2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum (*)

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) nr. 910/2014 frá 23. júlí 2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum og um niðurfellingu á tilskipun 1999/93/EB ([1]), einkum 3. mgr. 30. gr. og 2. mgr. 39. gr.,

og að teknu tilliti til eftirfarandi:

1) Í II. viðauka við reglugerð (ESB) nr. 910/2014 eru settar fram kröfur til fullgilds rafræns undirskriftarbúnaðar og fullgilds rafræns innsiglisbúnaðar.

2) Þar til bærar stofnanir á sviði stöðlunar annast það verkefni að semja tækniforskriftir, sem eru nauðsynlegar fyrir framleiðslu og setningu vara á markað, að teknu tilliti til tæknistigs á hverjum tíma.

3) Alþjóðlegu staðlasamtökin (ISO)/Alþjóðaraftækninefndin (IEC) fastsetja almenn hugtök og meginreglur um öryggi í upplýsingatækni og tilgreina almennt matslíkan sem leggja á til grundvallar mati á öryggiseiginleikum upplýsinga-tæknivara.

4) Staðlasamtök Evrópu (CEN) hafa, samkvæmt stöðlunarumboði M/460 frá framkvæmdastjórninni, þróað staðla fyrir fullgildan rafrænan undirskriftar- og innsiglisbúnað, þar sem rafrænu undirskriftargögnin eða rafrænu innsiglisgögnin eru geymd í umhverfi sem er að fullu, en ekki endilega eingöngu, stjórnað af notanda. Þessir staðlar teljast hentugir til að meta hvort slíkur búnaður sé í samræmi við viðeigandi kröfur sem settar eru fram í II. viðauka við reglugerð (ESB) nr. 910/2014.

5) Í II. viðauka við reglugerð (ESB) nr. 910/2014 er kveðið á um að aðeins fullgildur traustþjónustuveitandi megi stjórna rafrænum undirskriftargögnum fyrir hönd undirritanda. Öryggiskröfur og vottunarforskriftir vegna þeirra eru mismunandi eftir því hvort undirritandi hefur vöru í vörslu sinni eða fullgildur traustþjónustuveitandi er að verki fyrir hönd undirritanda. Til að taka á báðum aðstæðum og einnig til að ýta undir að með tímanum verði þróaðar vörur og matsstaðlar, sem henta fyrir tilteknar þarfir, ætti að tilgreina í viðaukanum við þessa ákvörðun staðla sem taka til beggja aðstæðna.

6) Þegar þessi ákvörðun framkvæmdastjórnarinnar er samþykkt bjóða nokkrir traustþjónustuveitendur þegar upp á lausnir til að stjórna rafrænum undirskriftargögnum fyrir hönd viðskiptavina sinna. Vottun vara er sem stendur takmörkuð við varbúnað (e. hardware security modules) sem vottaður er samkvæmt ólíkum stöðlum en er ekki enn sérstaklega vottaður með tilliti til krafna til fullgilds undirskriftar- og innsiglisbúnaðar. Enn eru þó ekki til útgefnir staðlar, eins og EN 419 211 (sem gildir um rafræna undirskrift myndaða í umhverfi sem er að fullu, en ekki endilega eingöngu, stjórnað af notanda), fyrir jafnmikilvægan markað vottaðra fjarvara (e. remote products). Þar eð verið er að þróa staðla, sem gætu átt við í þessum tilgangi, mun framkvæmdastjórnin bæta við þessa ákvörðun þegar slíkir staðlar eru tiltækir og teljast uppfylla kröfurnar sem settar eru fram í II. viðauka við reglugerð (ESB) nr. 910/2014. Þangað til skrá yfir slíka staðla er komið á fót er hægt að nota annað ferli við samræmismat slíkra vara með þeim skilyrðum sem kveðið er á um í b-lið 3 mgr. 30. gr. reglugerðar (ESB) nr. 910/2014.

7) Í viðaukanum er tilgreindur staðallinn EN 419 211 sem samanstendur af mismunandi hlutum (1–6) sem taka til mismunandi aðstæðna. Í hluta 5 og 6 í EN 419 211 eru viðbætur sem tengjast umhverfi fyrir fullgildan undirskriftarbúnað, s.s. tengingu við traustan undirskriftarbúnað. Vöruframleiðendum er frjálst að nota slíkar viðbætur.

(*) Þessi ESB-gerð birtist í Stjtíð. ESB L 109, 26.4.2016, bls. 40. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 167/2019 frá 13. júní 2019 um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) við EES-samninginn (bíður birtingar).

([1]) Stjtíð. ESB L 257, 28.8.2014, bls. 73.

Samkvæmt 56. forsendu reglugerðar (ESB) nr. 910/2014 takmarkast umfang vottunar skv. 30. og 39. gr. þeirrar reglugerðar við verndun undirskriftargagna og tekur ekki til hugbúnaðar sem myndar undirskrift.

8) Til að tryggja að rafrænar undirskriftir eða innsigli, mynduð með fullgildum undirskriftar- eða innsiglisbúnaði, séu varin gegn fölsun með áreiðanlegum hætti, eins og krafist er í II. viðauka við reglugerð (ESB) nr. 910/2014, eru hentug dulkóðunarreiknirit, lyklalengdir og tætiföll forsenda fyrir öryggi vottuðu vörunnar. Þar sem þetta mál hefur ekki verið samræmt á evrópskum vettvangi ættu aðildarríki að vinna saman að því að ná samkomulagi um dulkóðunarreiknirit, lyklalengdir og tætiföll til notkunar á sviði rafrænna undirskrifta og innsigla.

9) Samþykkt þessarar ákvörðunar úreldir ákvörðun framkvæmdastjórnarinnar 2003/511/EB ([1]). Því ber að fella hana úr gildi.

10) Ráðstafanirnar, sem kveðið er á um í þessari ákvörðun, eru í samræmi við álit nefndarinnar sem um getur í 48. gr. reglugerðar (ESB) nr. 910/2014.

SAMÞYKKT ÁKVÖRÐUN ÞESSA:

1. gr.

1. Í viðaukanum við þessa ákvörðun eru taldir upp staðlar fyrir öryggismat upplýsingatæknivara, sem gilda um vottun fullgilds rafræns undirskriftarbúnaðar eða fullgilds rafræns innsiglisbúnaðar skv. a-lið 3. mgr. 30. gr. eða 2. mgr. 39. gr. reglugerðar (ESB) nr. 910/2014, þar sem rafrænu undirskriftargögnin eða rafrænu innsiglisgögnin eru geymd í umhverfi sem er að fullu en ekki endilega eingöngu stjórnað af notanda.

2. Þar til framkvæmdastjórnin hefur tekið saman skrá yfir staðla fyrir öryggismat á upplýsingatæknivörum, sem gilda um vottun fullgilds rafræns undirskriftarbúnaðar eða fullgilds rafræns innsiglisbúnaðar, þar sem fullgildur traustþjónustuveitandi stjórnar rafrænu undirskriftargögnunum eða rafrænu innsiglisgögnunum fyrir hönd undirritanda eða aðila sem innsiglar, skal vottun slíkra vara byggjast á ferli sem, skv. b-lið 3. mgr. 30. gr., felur í sér öryggisstig sambærileg við þau sem krafist er í a-lið 3. mgr. 30. gr. og sem opinbera stofnunin eða einkaaðilinn, sem um getur í 1. mgr. 30. gr. reglugerðar (ESB) nr. 910/2014, hafa tilkynnt framkvæmdastjórninni um.

2. gr.

Ákvörðun 2003/511/EB er hér með felld úr gildi.

3. gr.

Ákvörðun þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Gjört í Brussel 25. apríl 2016.

Fyrir hönd framkvæmdastjórnarinnar,

Jean-Claude JUNCKER

forseti.

———

([1]) Ákvörðun framkvæmdastjórnarinnar 2003/511/EB frá 14. júlí 2003 um birtingu tilvísunarnúmera almennt viðurkenndra staðla fyrir vörur til rafrænna undirskrifta í samræmi við tilskipun Evrópuþingsins og ráðsins 1999/93/EB (Stjtíð. ESB L 175, 15.7.2003, bls. 45).

VIÐAUKI

SKRÁ YFIR STAÐLA SEM UM GETUR Í 1. MGR. 1. GR.

— *ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3*, eins og talið er upp hér á eftir:

  — *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,*

og

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

og

— ÍST EN 419 211 — Verndarsnið fyrir öruggan undirskriftarbúnað, hlutar 1–6 (Protection profiles for secure signature creation device, Parts 1 to 6), eftir því sem við á, eins og talið er upp hér á eftir:

  — ÍST EN 419211-1:2014 — Verndarsnið fyrir öruggan undirskriftarbúnað — Hluti 1: Yfirlit (Protection profiles for secure signature creation device — Part 1: Overview)

  — ÍST EN 419211-2:2013 — Verndarsnið fyrir öruggan undirskriftarbúnað — Hluti 2: Búnaður sem styðst við lyklamyndun (Protection Profile for Secure signature creation device — Part 2: Device with key generation)

  — ÍST EN 419211-3:2013 — Verndarsnið fyrir öruggan undirskriftarbúnað — Hluti 3: Búnaður sem styðst við lyklainnflutning (Protection Profile for Secure signature creation device — Part 2: Device with key generation)

  — ÍST EN 419211-4:2013 — Verndarsnið fyrir öruggan undirskriftarbúnað — Hluti 4: Viðbætur við tæki með lyklamyndun og trausta tengingu við skilríkjamyndunarbúnað (Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application)

  — ÍST EN 419211-5:2013 — Verndarsnið fyrir öruggan undirskriftarbúnað — Hluti 5: Viðbætur við tæki með lyklamyndun og trausta tengingu við undirskriftarbúnað (Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application)

  — ÍST EN 419211-6:2014 — Verndarsnið fyrir öruggan undirskriftarbúnað — Hluti 6: Viðbætur við tæki með lyklainnflutning og trausta tengingu við undirskriftarbúnað (Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application)