# KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2016/650,

## annettu 25 päivänä huhtikuuta 2016,

## hyväksyttyjen allekirjoituksen ja leiman luontivälineiden tietoturva-arviointia koskevien standardien vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 30 artiklan 3 kohdan ja 39 artiklan 2 kohdan mukaisesti

**(ETA:n kannalta merkityksellinen teksti)**

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta 23 päivänä heinäkuuta 2014 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 ([1]) ja erityisesti sen 30 artiklan 3 kohdan ja 39 artiklan 2 kohdan,

sekä katsoo seuraavaa:

(1) Asetuksen (EU) N:o 910/2014 liitteessä II vahvistetaan hyväksyttyjä sähköisen allekirjoituksen luontivälineitä ja hyväksyttyjä sähköisen leiman luontivälineitä koskevat vaatimukset.

(2) Standardointialalla toimivaltaisten organisaatioiden tehtävänä on laatia tekniset eritelmät, jotka ovat tarpeen tuotteiden tuotannon ja markkinoille saattamisen kannalta ja joissa otetaan huomioon teknologian nykyinen kehitysvaihe.

(3) ISO/IEC (Kansainvälinen standardisoimisjärjestö / Sähköalan kansainvälinen standardisointijärjestö) vahvistaa tietoturvallisuutta koskevat yleiset käsitteet ja periaatteet ja määrittelee yleisen arviointimallin, jota käytetään perustana tietotekniikkatuotteiden turvaominaisuuksien arvioinnissa.

(4) Euroopan standardointikomitea (CEN) on laatinut komission antaman standardointitoimeksiannon M/460 nojalla hyväksyttyjä sähköisen allekirjoituksen ja leiman luontivälineitä koskevat standardit, joiden mukaan sähköisen allekirjoituksen luontitiedot tai sähköisen leiman luontitiedot pidetään käyttäjän kokonaan muttei välttämättä yksinomaisesti hallinnoimassa ympäristössä. Näiden standardien katsotaan soveltuvan sen arviointiin, ovatko tällaiset välineet asetuksen (EU) N:o 910/2014 liitteessä II vahvistettujen asiaa koskevien vaatimusten mukaisia.

(5) Asetuksen (EU) N:o 910/2014 liitteen II mukaan ainoastaan hyväksytty luottamuspalvelun tarjoaja voi hallinnoida sähköisen allekirjoituksen luontitietoja allekirjoittajan puolesta. Tietoturvavaatimukset ja niiden sertifiointieritelmät ovat erilaiset, kun tuote on fyysisesti allekirjoittajan hallussa ja kun hyväksytty luottamuspalvelun tarjoaja toimii allekirjoittajan puolesta. Jotta voitaisiin ottaa huomioon molemmat tilanteet sekä suosia tiettyihin tarpeisiin soveltuvien tuotteiden ja arviointistandardien kehittämistä ajan mittaan, tämän päätöksen liitteessä olisi lueteltava standardit, jotka kattavat molemmat tilanteet.

(6) Tämän komission päätöksen hyväksymisajankohtana useat luottamuspalvelujen tarjoajat tarjoavat jo ratkaisuja sähköisen allekirjoituksen luontitietojen hallinnointiin asiakkaidensa puolesta. Tuotteiden sertifioinnit rajoittuvat tällä hetkellä turvalaitemoduuleihin, jotka sertifioidaan eri standardien perusteella, mutta joita ei vielä sertifioida hyväksyttyjä allekirjoituksen ja leiman luontivälineitä koskevien vaatimusten perusteella. Standardin EN 419 211 (jota sovelletaan sähköisiin allekirjoituksiin, jotka on luotu käyttäjän kokonaan muttei välttämättä yksinomaisesti hallinnoimassa ympäristössä) kaltaisia julkaistuja standardeja ei ole kuitenkaan vielä olemassa etäpalveluna tarjottaville sertifioiduille tuotteille, joiden markkinat ovat yhtä merkittävät. Koska tällaisiin tarkoituksiin mahdollisesti soveltuvia standardeja ollaan parhaillaan laatimassa, komissio täydentää tätä päätöstä, kunhan nämä standardit ovat saatavilla ja niiden on arvioitu olevan asetuksen (EU) N:o 910/2014 liitteessä II vahvistettujen vaatimusten mukaisia. Näiden standardien luettelon vahvistamiseen saakka tällaisten tuotteiden vaatimustenmukaisuuden arviointiin voidaan käyttää vaihtoehtoista prosessia asetuksen (EU) N:o 910/2014 30 artiklan 3 kohdan b alakohdassa säädetyin ehdoin.

(7) Liitteessä mainitaan standardi EN 419 211, joka koostuu useista osista (osat 1–6), jotka kattavat erilaisia tilanteita. Standardin EN 419 211 osissa 5 ja 6 määritellään hyväksyttyjen allekirjoituksen luontivälineiden ympäristöön

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

liittyviä laajennuksia, kuten tiedonvaihto luotettujen allekirjoituksen luontisovellusten kanssa. Tuotteiden valmistajat voivat vapaasti soveltaa näitä laajennuksia. Asetuksen (EU) N:o 910/2014 johdanto-osan 56 kappaleen mukaan mainitun asetuksen 30 ja 39 artiklan nojalla tehtyjen sertifiointien soveltamisala rajoittuu allekirjoituksen luontitietojen suojaamiseen, ja allekirjoituksen luontisovellukset jätetään sertifioinnin soveltamisalan ulkopuolelle.

(8) Sen varmistamiseksi, että hyväksytyllä allekirjoituksen tai leiman luontivälineellä luodut sähköiset allekirjoitukset tai leimat on luotettavasti suojattu väärentämiseltä, kuten asetuksen (EU) N:o 910/2014 liitteessä II edellytetään, soveltuvat salausalgoritmit, avaimen pituudet ja hajautusfunktiot ovat sertifioidun tuotteen turvallisuuden välttämätön edellytys. Koska tätä näkökohtaa ei ole yhdenmukaistettu Euroopan tasolla, jäsenvaltioiden olisi yhteistyössä sovittava sähköisten allekirjoitusten ja leimojen alalla käytettävistä salausalgoritmeista, avaimen pituuksista ja hajautusfunktioista.

(9) Tämän päätöksen hyväksymisen myötä komission päätös 2003/511/EY ([1]) vanhentuu. Se olisi sen vuoksi kumottava.

(10) Tässä päätöksessä säädetyt toimenpiteet ovat asetuksen (EU) N:o 910/2014 48 artiklassa tarkoitetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

*1 artikla*

1. Tämän päätöksen liitteessä luetellaan tietoteknisten tuotteiden tietoturva-arviointia koskevat standardit, joita sovelletaan hyväksyttyjen sähköisen allekirjoituksen luontivälineiden tai hyväksyttyjen sähköisen leiman luontivälineiden sertifiointiin asetuksen (EU) N:o 910/2014 30 artiklan 3 kohdan a alakohdan tai 39 artiklan 2 kohdan mukaisesti, kun sähköisen allekirjoituksen luontitiedot tai sähköisen leiman luontitiedot pidetään käyttäjän kokonaan muttei välttämättä yksinomaisesti hallinnoimassa ympäristössä.

2. Siihen saakka, kunnes komissio vahvistaa luettelon tietoteknisten tuotteiden tietoturva-arviointia koskevista standardeista, joita sovelletaan hyväksyttyjen sähköisen allekirjoituksen luontivälineiden tai hyväksyttyjen sähköisen leiman luontivälineiden sertifiointiin, kun hyväksytty luottamuspalvelun tarjoaja hallinnoi sähköisen allekirjoituksen luontitietoja tai sähköisen leiman luontitietoja allekirjoittajan tai leiman luojan puolesta, tällaisten tuotteiden sertifiointi perustuu prosessiin, jossa käytetään 30 artiklan 3 kohdan b alakohdan mukaisesti 30 artiklan 3 kohdan a alakohdassa vaadittujen tasojen kanssa vertailukelpoisia tietoturvatasoja ja josta asetuksen (EU) N:o 910/2014 30 artiklan 1 kohdassa tarkoitettu julkinen tai yksityinen taho on ilmoittanut komissiolle.

*2 artikla*

Kumotaan päätös 2003/511/EY.

*3 artikla*

Tämä päätös tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tehty Brysselissä 25 päivänä huhtikuuta 2016.

*Komission puolesta*

*Puheenjohtaja*

Jean-Claude JUNCKER

([1]) Komission päätös 2003/511/EY, tehty 14 päivänä heinäkuuta 2003, sähköisiin allekirjoituksiin liittyviä tuotteita koskevien yleisesti tunnustettujen standardien viitenumeroiden julkaisemisesta Euroopan parlamentin ja neuvoston direktiivin 1999/93/EY mukaisesti (EUVL L 175, 15.7.2003, s. 45).

*LIITE*

**LUETTELO 1 ARTIKLAN 1 KOHDASSA TARKOITETUISTA STANDARDEISTA**

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

  — 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

  ja

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

  ja

— EN 419 211 – Protection profiles for secure signature creation device, osat 1–6 – tarpeen mukaan – seuraavasti:

  — 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