Euroopan unionin
virallinen lehti

FI
L-sarja

2025/2392

1.12.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/2392,

annettu 28 päivänä marraskuuta 2025,

Euroopan parlamentin ja neuvoston asetuksessa (EU) 2024/2847 tarkoitettujen digitaalisia elementtejä sisältävien tärkeiden ja kriittisten tuotteiden ryhmien teknisestä kuvauksesta

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) 23 päivänä lokakuuta 2024 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/2847 ([1]) ja erityisesti sen 7 artiklan 4 kohdan,

sekä katsoo seuraavaa:

(1) Asetuksella (EU) 2024/2847 säädetään digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuutta koskevista säännöistä. Kyseisen asetuksen liitteessä III vahvistetaan digitaalisia elementtejä sisältävien tärkeiden tuotteiden ryhmät, joihin sovelletaan markkinoille saatettaessa tiukempia vaatimustenmukaisuuden arviointimenettelyjä kuin muihin digitaalisia elementtejä sisältäviin tuotteisiin. Asetuksen (EU) 2024/2847 liitteessä IV vahvistetaan digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmät, joiden osalta valmistajia voitaisiin edellyttää hankkimaan eurooppalainen kyberturvallisuussertifikaatti Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 ([2]) mukaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän puitteissa tai joille olisi tehtävä pakollinen kolmannen osapuolen suorittama vaatimustenmukaisuuden arviointi markkinoille saatettaessa.

(2) Asetuksen (EU) 2024/2847 7 artiklan 1 kohdan ja 8 artiklan 1 kohdan mukaan digitaalisia elementtejä sisältävän tuotteen ydintoiminto määrittää, vastaako kyseinen digitaalisia elementtejä sisältävä tuote digitaalisia elementtejä sisältävien tärkeiden tai kriittisten tuotteiden ryhmän teknistä kuvausta ja sovelletaanko siihen tämän vuoksi niitä koskevia vaatimustenmukaisuuden arviointimenettelyjä.

(3) Kehittäessään digitaalisia elementtejä sisältävää tuotetta ja saavuttaakseen halutut toiminnot valmistajat tyypillisesti integroivat omiin digitaalisia elementtejä sisältäviin tuotteisiinsa muita komponentteja, jotka ovat niin ikään digitaalisia elementtejä sisältäviä tuotteita ja jotka saattavat vastata tärkeiden tai kriittisten tuotteiden ryhmän teknistä kuvausta. Asetuksen (EU) 2024/2847 nojalla digitaalisia elementtejä sisältävään tuotteeseen sovelletaan digitaalisia elementtejä sisältäviin tärkeisiin tai kriittisiin tuotteisiin sovellettavia vaatimustenmukaisuuden arviointimenettelyjä, jos kyseinen tuote kokonaisuudessaan on kyseisen asetuksen liitteissä III ja IV tarkoitettu tärkeä tai kriittinen tuote. Esimerkiksi sulautetun selaimen integrointi älypuhelimissa käytettävän uutissovelluksen komponentiksi ei sinänsä johda siihen, että uutissovellukseen sovelletaan vaatimustenmukaisuuden arviointimenettelyä, jota sovelletaan digitaalisia elementtejä sisältäviin tuotteisiin, joiden ydintoiminto on ”erilliset ja sulautetut selaimet”. Asetuksen (EU) 2024/2847 mukaisesti valmistajan on kuitenkin varmistettava, että digitaalisia elementtejä sisältävä tuote kokonaisuudessaan täyttää olennaiset kyberturvallisuusvaatimukset. Sen vuoksi valmistajan on arvioitava koko tuotteen turvallisuus ottamalla tarvittaessa huomioon siihen integroitujen komponenttien tai toimintojen turvallisuuden. Jotta esimerkiksi uutissovelluksen valmistaja voi osoittaa, että sen digitaalisia elementtejä sisältävä tuote on asetuksen (EU) 2024/2847 mukainen, valmistajan on osoitettava, että uutissovellus kokonaisuudessaan täyttää sovellettavat vaatimukset, ottamalla tarvittaessa huomioon sovellukseen integroidun sulautetun selaimen turvallisuuden.

([1]) EUVL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Se, että digitaalisia elementtejä sisältävä tuote suorittaa muita kuin tässä asetuksessa vahvistetuissa teknisissä kuvauksissa esitettyjä toimintoja tai niiden lisäksi myös muita toimintoja, ei itsessään merkitse sitä, että digitaalisia elementtejä sisältävällä tuotteella ei ole jonkin asetuksen (EU) 2024/2847 liitteissä III ja IV tarkoitetun tuoteryhmän ydintoimintoa. Esimerkiksi digitaalisia elementtejä sisältävissä tuotteissa, joilla on ”käyttöjärjestelmien” ydintoiminto, on usein kyseisen tuoteryhmän tekniseen kuvaukseen sisältymättömiä oheistoimintoja suorittavia ohjelmia, kuten laskimia tai yksinkertaisia grafiikkaohjelmia. Digitaalisia elementtejä sisältävissä tuotteissa on usein myös komponentteja, joilla on toisen digitaalisia elementtejä sisältävän tärkeän tai kriittisen tuotteen toiminto, esimerkkeinä käyttöjärjestelmä, joka sisältää selaintoiminnon, tai reititin, johon on integroitu palomuuritoiminto. Tämä ei kuitenkaan itsessään tarkoita sitä, että tällaisilla digitaalisia elementtejä sisältävillä tuotteilla ei olisi ”käyttöjärjestelmien” tai ”reitittimien, internetyhteyden muodostamiseen tarkoitettujen modeemien sekä kytkimien” ydintoimintoa.

(5) Toisaalta digitaalisia elementtejä sisältävän tuotteen, joka pystyy suorittamaan jonkin asetuksen (EU) 2024/2847 liitteissä III ja IV tarkoitetun tuoteryhmän toimintoja mutta jonka varsinainen ydintoiminto eroaa tällaisen tuoteryhmän ydintoiminnosta, ei katsota täyttävän kyseisen tuoteryhmän teknistä kuvausta. Esimerkiksi SOAR-ohjelma (tietoturvan orkestrointi, automatisointi ja tietoturvahäiriöön vastaaminen) pystyy usein suorittamaan ryhmään ”tietoturvatietojen ja tapahtumien hallintajärjestelmät (SIEM)” kuuluvien digitaalisia elementtejä sisältävien tuotteiden toiminnot eli keräämään dataa, analysoimaan sitä ja esittämään sen käyttökelpoisena tietona turvallisuuteen liittyviä tarkoituksia varten. Koska SOAR-ohjelman ydintoiminto ei kuitenkaan ole sama kuin SIEM-järjestelmällä, sen ei yleisesti ottaen katsota vastaavan ryhmän ”tietoturvatietojen ja tapahtumien hallintajärjestelmät (SIEM)” teknistä kuvausta. Vastaavasti älypuhelin sisältää tyypillisesti komponentteja, jotka suorittavat useiden asetuksen (EU) 2024/2847 liitteissä III ja IV tarkoitettujen tuoteryhmien, kuten käyttöjärjestelmän tai integroidun salasanojen hallinnointityökalun, toimintoja. Koska älypuhelimen ydintoiminto ei kuitenkaan ole käyttöjärjestelmä tai salasanojen hallinnointityökalu, sen ei yleisesti ottaen katsota vastaavan näiden tuoteryhmien teknistä kuvausta.

(6) Asetuksen (EU) 2024/2847 13 artiklan 2 ja 3 kohdan mukaan digitaalisia elementtejä sisältävien tuotteiden valmistajien on pantava täytäntöön asetuksen (EU) 2024/2847 liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset tavalla, joka on oikeassa suhteessa digitaalisia elementtejä sisältävän tuotteen riskeihin, perustuen digitaalisia elementtejä sisältävän tuotteen käyttötarkoitukseen ja kohtuudella ennakoitavissa olevaan käyttöön sekä käyttöolosuhteisiin ja ottaen huomioon aika, jona tuotteen odotetaan olevan käytössä. Kyseisen asetuksen 13 artiklan 2 ja 3 kohdan mukaisesti ja riippumatta siitä, katsotaanko digitaalisia elementtejä sisältävä tuote tärkeäksi tai kriittiseksi digitaalisia elementtejä sisältäväksi tuotteeksi, valmistajien on tehtävä kattava kyberturvallisuusriskien arviointi ja ilmoitettava, millä tavalla olennaiset kyberturvallisuusvaatimukset on pantu täytäntöön riskinarvioinnin perusteella, mukaan lukien niiden testaus ja varmuus. Jos digitaalisia elementtejä sisältävän tuotteen ydintoiminto vastaa digitaalisia elementtejä sisältävän tärkeän tai kriittisen tuotteen teknistä kuvausta, valmistajien on osoitettava vaatimustenmukaisuus asetuksen (EU) 2024/2847 32 artiklan 2, 3, 4 ja 5 kohdassa vahvistettujen erityisten vaatimustenmukaisuuden arviointimenettelyjen mukaisesti.

(7) Tämä asetus sisältää esimerkkejä digitaalisia elementtejä sisältävistä tuotteista, joiden ydintoiminto vastaa tiettyjen digitaalisia elementtejä sisältävien tärkeiden tai kriittisten tuotteiden teknistä kuvausta. Esimerkkejä annetaan ainoastaan havainnollistamistarkoituksessa, eivätkä ne muodosta tyhjentävää luetteloa.

(8) Jotta valmistajille voidaan taata oikeusvarmuus, digitaalisia elementtejä sisältävät tuoteryhmät, joihin kuuluvat tuotteet ovat väärinkäytöltä suojattuja mikroprosessoreita, väärinkäytöltä suojattuja mikro-ohjaimia ja älykortteja tai vastaavia laitteita, mukaan lukien turvaelementit, olisi erotettava toisistaan sen mukaan, minkä tasoisesti ne on suunniteltu suojautumaan puutteiden tai heikkouksien potentiaaliselta väärinkäytöltä. AVA_VAN-taso on laajalti käytetty ja standardoitu tapa ilmaista tällainen suojautumiskyky. AVA_VAN-tasot on vahvistettu julkisesti saatavilla olevissa yhteisiä arviointikriteereitä (Common Criteria) ja yhteisiä arviointimenetelmiä (Common Evaluation Methodology) koskevissa standardeissa, joihin pohjautuvat markkinoilla laajalti käytössä olevat sertifiointikehykset,

kuten komission täytäntöönpanoasetus (EU) 2024/482 ([3]). Täytäntöönpanoasetuksessa (EU) 2024/482 vahvistetaan eurooppalainen kyberturvallisuuden sertifiointijärjestelmä, joka mahdollistaa tuotteen sertifioinnin sen varmuustason perusteella. Maailmanlaajuisten käytäntöjen mukaisesti täytäntöönpanoasetuksessa (EU) 2024/482 säädetään mahdollisuudesta myöntää standardien vanhempiin versioihin perustuvia sertifikaatteja vuoden 2027 loppuun saakka. Näin ollen asetuksen (EU) 2024/2847 puitteissa on aiheellista sallia, että AVA_VAN-tasot ilmaistaan viittaamalla joko kyseisten standardien viimeisimpään versioon tai vanhempiin versioihin.

(9) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EU) 2024/2847 62 artiklan 1 kohdalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) ’yhteisillä kriteereillä’ (Common Criteria) tietotekniikan turvallisuuden arviointia koskevia yhteisiä kriteereitä sellaisina kuin ne on määritelty täytäntöönpanoasetuksen (EU) 2024/482 2 artiklan 1 kohdassa tai vahvistettu kyseisen täytäntöönpanoasetuksen 3 artiklan 2 kohdan a ja b alakohdassa tarkoitetuissa standardeissa;

2) ’yhteisillä arviointimenetelmillä’ (Common Evaluation Methodology) tietoteknologian turvallisuuden arviointia koskevia yhteisiä menetelmiä sellaisina kuin ne on määritelty täytäntöönpanoasetuksen (EU) 2024/482 2 artiklan 2 kohdassa tai vahvistettu kyseisen täytäntöönpanoasetuksen 3 artiklan 2 kohdan c ja d alakohdassa tarkoitetuissa standardeissa.

2 artikla

1. Asetuksen (EU) 2024/2847 liitteessä III lueteltuihin luokkiin I ja II kuuluvien digitaalisia elementtejä sisältävien tuotteiden ryhmien tekniset kuvaukset vahvistetaan tämän asetuksen liitteessä I.

2. Asetuksen (EU) 2024/2847 liitteessä IV lueteltujen digitaalisia elementtejä sisältävien tuotteiden ryhmien tekniset kuvaukset vahvistetaan tämän asetuksen liitteessä II.

3 artikla

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

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 28 päivänä marraskuuta 2025.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

([3]) Komission täytäntöönpanoasetus (EU) 2024/482, annettu 31 päivänä tammikuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä (EUVL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

LIITE I

DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVÄT TÄRKEÄT TUOTTEET

I luokka

Tuoteryhmä	Tekninen kuvaus
1. Identiteetinhallintajärjestelmät ja korotettujen käyttöoikeuksien hallintaohjelmistot ja -laitteistot, mukaan lukien todennuksessa sekä kulunvalvonnassa käytettävät lukijat, myös biometriset lukijat	Identiteetinhallintajärjestelmät ovat digitaalisia elementtejä sisältäviä tuotteita, jotka tarjoavat mekanismeja todentamista tai valtuutusta varten. Ne voivat myös tarjota mekanismeja luonnollisten henkilöiden, oikeushenkilöiden, laitteiden tai järjestelmien tunnistetietojen elinkaarihallintaan, kuten tunnistetietojen rekisteröintiin, luomiseen, ylläpitoon tai rekisteristä poistamiseen. Näihin järjestelmiin kuuluvat myös pääsynhallintajärjestelmät, joilla valvotaan luonnollisten henkilöiden, oikeushenkilöiden, laitteiden tai järjestelmien pääsyä digitaalisiin resursseihin tai fyysisiin paikkoihin. Korotettujen käyttöoikeuksien hallintaohjelmisto on pääsynhallintajärjestelmä, jolla valvotaan ja seurataan tietoteknisten tai operatiivisen teknologian järjestelmien ja arkaluonteisten tietojen käyttöoikeuksia organisaation sisällä, mukaan lukien järjestelmät, joilla pannaan täytäntöön etuoikeutettuja käyttäjiä koskevia eriytettyjä pääsynvalvontamenettelyjä. Tähän ryhmään kuuluvat muun muassa todentamiseen ja kulunvalvontaan tarkoitetut lukijat, biometriset lukijat, kertakirjautumisohjelmistot, yhteisen käyttäjäntunnistuksen ohjelmistot, kertakäyttöisen salasanan generoivat ohjelmistot ja tunnistuslaitteistot, kuten maksutapahtuman tunnistusnumerogeneraattorit, tunnistautumisen ohjelmistot ja monivaiheisen tunnistautumisen ohjelmistot.
2. Erilliset ja sulautetut selaimet	Digitaalisia elementtejä sisältävät ohjelmistotuotteet, joiden avulla loppukäyttäjät voivat päästä verkkosisältöihin ja -palveluihin, hahmontaa ja olla vuorovaikutuksessa niiden kanssa internetiin ja muihin verkkoihin liitetyillä palvelimilla. Niihin kuuluvat tyypillisesti verkkoselain, joka lukee ja esittää merkintäkielellä kirjoitettua sisältöä (kuten HTML), verkkoprotokollien (kuten HTTP ja HTTPS) tuki, kyky suorittaa komentosarjoja ja hallita käyttäjien syötteitä sekä verkkosivustoilta peräisin olevan väliaikaisen tai pysyvän datan säilyttäminen (evästeet). Tähän luokkaan kuuluvat muun muassa erilliset sovellukset, jotka suorittavat selainten toimintoja, toiseen järjestelmään tai sovellukseen integroitavaksi tarkoitetut sulautetut selaimet ja selaimet, joihin on integroitu tekoälyagentti.
3. Salasanojen hallinnointityökalut	Digitaalisia elementtejä sisältävät tuotteet, jotka tallentavat salasanoja paikalliselle laitteelle tai etäpalvelimelle, mukaan lukien muun muassa salasanojen generointi sekä salasanojen jakaminen ja integrointi paikallisten tai kolmannen osapuolen sovellusten kanssa salasanojen käyttöä varten. Tähän ryhmään kuuluvat muun muassa paikalliset salasanojen hallinnointityökalut, selainlaajennuksina tarjottavat salasanojen hallinnointityökalut, yritysten salasanojen hallinnointityökalut sekä laitteistopohjaiset salasanojen hallinnointityökalut.

Tuoteryhmä	Tekninen kuvaus
4. Ohjelmistot, jotka etsivät, poistavat tai siirtävät karanteeniin haittaohjelmistoja	Digitaalisia elementtejä sisältävät ohjelmistotuotteet, joista käytetään yleensä nimitystä virustorjuntaohjelma tai haittaohjelmien torjuntaohjelma ja jotka havaitsevat tai etsivät laitteilta haittaohjelmia tai -koodia tai poistavat tällaiset ohjelmat tai koodit tai siirtävät ne karanteeniin laitteiden eheyden, tietoturvan tai saatavuuden säilyttämiseksi. Tässä tuoteryhmässä haittaohjelmilla tarkoitetaan ohjelmistoja, jotka sisältävät haitallisia ominaisuuksia tai toimintoja, jotka voivat aiheuttaa suoraan tai välillisesti haittaa käyttäjälle ja/tai tietokonejärjestelmälle, kuten viruksia, matoja, kiristysohjelmia, vakoiluohjelmia ja troijalaisia. Tähän ryhmään kuuluvat muun muassa ohjelmistot, jotka havaitsevat tai etsivät haittaohjelmia reaaliaikaisesti tai manuaalisesti, sekä rootkit-suojaukset ja pelastuslevyt, joiden ydintoiminto on haittaohjelmien etsiminen, poistaminen tai siirtäminen karanteeniin.
5. Digitaalisia elementtejä sisältävät tuotteet, joissa on virtuaalisen yksityisverkon (VPN) toiminto	Digitaalisia elementtejä sisältävät tuotteet, joilla luodaan salattu looginen tunneli fyysisen tai virtuaalisen verkon järjestelmäresurssien avulla. Tähän ryhmään kuuluvat muun muassa VPN-asiakkaat, -palvelimet ja -yhdyskäytävät.
6. Verkonhallintajärjestelmät	Digitaalisia elementtejä sisältävät tuotteet, joilla hallitaan verkkoon liitettyjä elementtejä, kuten palvelimia, reitittimiä, kytkimiä, työasemia, tulostimia tai mobiililaitteita, seuraamalla niitä ja ohjaamalla niiden verkkotoimintoja ja konfiguraatiota. Tähän luokkaan kuuluvat muun muassa päästä päähän -hallintajärjestelmät ja erityiset konfiguraation hallintajärjestelmät, kuten ohjelmisto-ohjattujen verkkojen ohjaimet.
7. Tietoturvatietojen ja tapahtumien hallintajärjestelmät (SIEM)	Digitaalisia elementtejä sisältävät tuotteet, jotka keräävät tietoja useista lähteistä, analysoivat ja korreloivat näitä tietoja ja esittävät ne käyttökelpoisina tietoina turvallisuuteen liittyviä tarkoituksia, kuten uhkien ja poikkeamien havaitsemista, rikosteknistä analyysia tai vaatimustenmukaisuuden varmistamista varten.
8. Käynnistysohjelmat	Digitaalisia elementtejä sisältävät ohjelmistotuotteet, jotka hallinnoivat järjestelmän käynnistymisprosessia virran kytkemisen tai uudelleenkäynnistyksen jälkeen alustamalla laitteiston, lataamalla tai siirtämällä hallinnan käyttöjärjestelmäympäristöön tai järjestelmäresursseille ja valitsemalla käynnistysvaihtoehdot. Tähän ryhmään kuuluvat muun muassa UEFI-laiteohjelmisto sekä yksi- ja monivaiheiset käynnistyslataajat.
9. Julkisen avaimen infrastruktuuri ja digitaalisen varmenteen luomiseen käytettävät ohjelmistot	Digitaalisia elementtejä sisältävät tuotteet, joita käytetään osana julkisen avaimen infrastruktuuria (PKI), joka hallinnoi digitaalisten varmenteiden validointia, luomista, myöntämistä, jakelua, tilan julkaisemista, uusimista tai peruuttamista taikka digitaalisiin varmenteisiin liittyvien salausavainten generointia, säilyttämistä, talletusta, vaihtoa, hävittämistä tai kiertoa. Tähän ryhmään kuuluvat muun muassa avaintenhallinnan järjestelmät, digitaalisten varmenteiden hallintajärjestelmät, verkossa olevat varmenteen statusprotokollat (OCSP-vastaajat) ja all-in-one-PKI-ratkaisut.

Tuoteryhmä	Tekninen kuvaus
10. Fyysiset ja virtuaaliset verkkorajapinnat	Fyysiset verkkorajapinnat ovat digitaalisia elementtejä sisältäviä tuotteita, jotka yhdistävät laitteen suoraan verkkoon yleensä datayhteyskerroksessa toimivien rajapinta-ajureiden tarjoaman ohjelmointirajapinnan (API) kautta ja joissa on laitesovittimia siirtoväyliin ja niitä vastaavat laiteohjelmistot, jotka toimivat tyypillisesti fyysisessä ja datayhteyskerroksessa. Virtuaaliset verkkorajapinnat ovat digitaalisia elementtejä sisältäviä tuotteita, jotka suoraan tai epäsuorasti yhdistävät laitteen verkkoon ohjelmointirajapinnan kautta, joka jäljittelee tyypillisesti datayhteyskerroksessa toimivien fyysisen verkkoliitännän ajureiden rajapintaa. Tähän ryhmään kuuluvat muun muassa kiinteät ja langattomat verkkokortit, ohjaimet ja sovittimet, kuten Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee tai Fieldbus, sekä puhtaasti virtuaaliset erilliset tuotteet, kuten virtuaaliset verkkokortit sekä CNI- ja VPN-rajapinnat.
11. Käyttöjärjestelmät	Digitaalisia elementtejä sisältävät ohjelmistotuotteet, jotka tarjoavat taustalla olevan laitteiston abstraktin rajapinnan ja ohjaavat ohjelmistojen suorittamista ja joiden toimintoihin voi kuulua esimerkiksi laskentaresurssien hallinta ja konfiguraatio, ajoituksen hallinta, syötön ja tulostuksen ohjaus, datan hallinta sekä rajapinta, jonka kautta sovellukset voivat olla vuorovaikutuksessa järjestelmäresurssien ja oheislaitteiden kanssa. Tähän ryhmään kuuluvat muun muassa reaaliaikaiset käyttöjärjestelmät, yleiskäyttöjärjestelmät ja erityiskäyttöjärjestelmät.
12. Reitittimet, internetyhteyden muodostamiseen tarkoitetut modeemit sekä kytkimet	Reitittimet ovat digitaalisia elementtejä sisältäviä tuotteita, jotka luovat ja ohjaavat tiedonkulkua eri verkkojen välillä valitsemalla polkuja tai reittejä käyttämällä reititysprotokollamekanismeja ja algoritmeja ja jotka toimivat tyypillisesti datayhteyskerroksessa. Tähän ryhmään kuuluvat muun muassa kiinteät ja langattomat reitittimet ja virtuaalireitittimet sekä modeemi- ja muut reitittimet.
	Internetyhteyden muodostamista varten tarkoitetut modeemit ovat digitaalisia elementtejä sisältäviä laitteistotuotteita, joissa käytetään digitaalista modulaatio- ja demodulaatiotekniikkaa analogisten signaalien muuntamiseen digitaalisista signaaleista ja digitaalisiksi signaaleiksi IP-pohjaista viestintää varten. Tähän ryhmään kuuluvat muun muassa kuitumodeemit, DSL-modeemit, kaapelimodeemit (DOCSIS), satelliittimodeemit ja matkapuhelinmodeemit.
	Kytkimet ovat digitaalisia elementtejä sisältäviä tuotteita, jotka luovat yhteyden verkkoon liitettyjen laitteiden välille datapakettien välitysmekanismien avulla ja joilla on hallintataso, joka yleensä toteutetaan datayhteys- tai verkkokerroksessa. Tähän luokkaan kuuluvat muun muassa hallittavat kytkimet, älykytkimet, monikerroksiset kytkimet, virtuaaliset turvakytkimet, ohjelmoitavat kytkimet ohjelmisto-ohjattuja verkkoja ja siltoja, kuten langattomia tukiasemia, varten.

Tuoteryhmä	Tekninen kuvaus
13. Mikroprosessorit, joissa on turvallisuustoimintoja	Digitaalisia elementtejä sisältävät tuotteet, jotka ovat mikropiirejä, jotka suorittavat keskusprosessointitoimintoja käyttämällä ulkoista muistia ja oheislaitteita, mukaan lukien mikrokäsky ja muut matalan tason laiteohjelmistot. Lisäksi ne tarjoavat turvallisuustoimintoja, joihin kuuluvat muun muassa salaus, todentaminen, suojattu avainten säilytys, satunnaisnumeroiden generointi, luotettu suoritusympäristö tai muita laitteistoperusteisia suojausmekanismeja, joilla pyritään turvaamaan muita tuotteita, verkkoja tai palveluita kuin mikroprosessori itse, kuten suojattu käynnistysketju, virtualisointi tai suojatut viestintärajapinnat.
14. Mikro-ohjaimet, joissa on turvallisuustoimintoja	Digitaalisia elementtejä sisältävät tuotteet, jotka ovat keskusprosessointitoimintoja suorittavia mikropiirejä, jotka sisältävät mikroprosessorin ohjelmoinnin mahdollistavan integroidun muistin ja yleensä myös muita oheislaitteita, mukaan lukien mikrokäsky ja muut matalan tason laiteohjelmistot. Lisäksi ne tarjoavat turvallisuustoimintoja, joihin kuuluvat muun muassa salaus, todentaminen, suojattu avainten säilytys, satunnaisnumeroiden generointi, luotettu suoritusympäristö tai muita laitteistoperusteisia suojausmekanismeja, joilla pyritään turvaamaan muita tuotteita, verkkoja tai palveluita kuin mikro-ohjain itse, kuten suojattu käynnistysketju, virtualisointi tai suojatut viestintärajapinnat.
15. Sovelluskohtaiset integroidut piirit (ASIC) ja kenttäohjelmoitavat porttimatriisit (FPGA), joissa on turvallisuustoimintoja	Turvallisuustoimintoja sisältävät sovelluskohtaiset mikropiirit (ASIC) ovat digitaalisia elementtejä sisältäviä tuotteita, jotka ovat mikropiirejä ja jotka on kokonaisuudessaan tai osittain suunniteltu suorittamaan tietty toiminto tai toteuttamaan tietty sovellus, mukaan lukien mikrokäsky ja muut matalan tason laiteohjelmistot. Lisäksi ne tarjoavat turvallisuustoimintoja, joihin kuuluvat muun muassa salaus, todentaminen, suojattu avainten säilytys, satunnaisnumeroiden generointi, luotettu suoritusympäristö tai muita laitteistoperusteisia suojausmekanismeja, joilla pyritään turvaamaan muita tuotteita, verkkoja tai palveluita kuin ASIC itse, kuten suojattu käynnistysketju, virtualisointi tai suojatut viestintärajapinnat.
	Turvallisuustoimintoja sisältävät kenttäohjelmoitavat porttimatriisit (FPGA) ovat digitaalisia elementtejä sisältäviä tuotteita, jotka ovat mikropiirejä. Niiden piirteisiin kuuluu konfiguroitavien logiikkalohkojen matriisi, ja ne on suunniteltu siten, että ne voidaan ohjelmoida uudelleen valmistuksen jälkeen suorittamaan tietty toiminto tai toteuttamaan tietty sovellus, mukaan lukien mikrokäsky ja muut matalan tason laiteohjelmistot. Lisäksi ne tarjoavat turvallisuustoimintoja, joihin kuuluvat muun muassa salaus, todentaminen, suojattu avainten säilytys, satunnaisnumeroiden generointi, luotettu suoritusympäristö tai muita laitteistoperusteisia suojausmekanismeja, joilla pyritään turvaamaan muita tuotteita, verkkoja tai palveluita kuin FPGA itse, kuten suojattu käynnistysketju, virtualisointi tai suojatut viestintärajapinnat.
16. Älykodin yleiskäyttöiset virtuaaliavustajat	Digitaalisia elementtejä sisältävät tuotteet, jotka kommunikoivat julkisessa internetissä joko suoraan tai muiden laitteiden kautta ja jotka käsittelevät luonnolliseen kieleen perustuvia pyyntöjä, tehtäviä tai kysymyksiä, jotka on esitetty ääneen tai kirjallisessa muodossa, ja jotka näiden pyyntöjen, tehtävien tai kysymysten perusteella tarjoavat pääsyn muihin palveluihin tai hallinnoivat verkkoon liitettyjen laitteiden toimintoja asuinympäristöissä. Tähän ryhmään kuuluvat muun muassa älykaiuttimet, joissa on integroitu virtuaaliavustaja, ja erilliset virtuaaliavustajat, jotka vastaavat tätä kuvausta.

Tuoteryhmä	Tekninen kuvaus
17. Älykodin tuotteet, joissa on turvallisuustoimintoja, mukaan lukien ovien älylukot, turvakamerat, itkuhälyttimet ja hälytysjärjestelmät	Digitaalisia elementtejä sisältävät tuotteet, joilla suojellaan kuluttajien fyysistä turvallisuutta asuinympäristössä ja joita voidaan valvoa tai hallinnoida etäältä muiden järjestelmien avulla, sekä laitteistot ja ohjelmistot, joilla tällaisia tuotteita hallitaan keskitetysti. Tähän ryhmään kuuluvat muun muassa ovien älylukot, itkuhälytinjärjestelmät, hälytysjärjestelmät ja kodin turvakamerat.
18. Euroopan parlamentin ja neuvoston direktiivin 2009/48/EY ([1]) soveltamisalaan kuuluvat verkkoon liitetyt lelut, joissa on vuorovaikutustoimintoja (esimerkiksi puhe tai kuvaaminen) tai paikannustoimintoja	Internetiin liitetyt lelut, joissa on vuorovaikutustoimintoja, ovat direktiivin 2009/48/EY soveltamisalaan kuuluvia digitaalisia elementtejä sisältäviä tuotteita, jotka kommunikoivat julkisessa internetissä joko suoraan tai muiden laitteiden kautta ja joissa on sisäänrakennettua teknologiaa, joka mahdollistaa saapuvan ja lähtevän viestinnän, kuten näppäimistö, mikrofoni, kaiutin tai kamera.
	Internetiin liitetyt lelut, joissa on paikannustoimintoja, ovat direktiivin 2009/48/EY soveltamisalaan kuuluvia digitaalisia elementtejä sisältäviä tuotteita, jotka kommunikoivat julkisessa internetissä joko suoraan tai muiden laitteiden kautta ja joissa on teknologiaa, joka mahdollistaa lelun tai sen käyttäjän maantieteellisen sijainnin seurannan tai päättelyn. Jos lelu ainoastaan havaitsee käyttäjän tai muiden lelujen läheisyyden anturitekniikan avulla, lelussa ei katsota olevan sijainninseurantatoimintoja.
19. Henkilökohtaiset puettavat tuotteet, joita pidetään yllä tai jotka sijoitetaan ihmiskeholle ja joita käytetään terveyden monitorointiin (kuten seurantaan) ja joihin ei sovelleta Euroopan parlamentin ja neuvoston asetusta (EU) 2017/745 ([2]) tai Euroopan parlamentin ja neuvoston asetusta (EU) 2017/746 ([3]), tai henkilökohtaiset puettavat tuotteet, jotka on tarkoitettu lasten käyttöön ja käytettäväksi lapsilla.	Henkilökohtaiset puettavat tuotteet, joita pidetään yllä tai jotka sijoitetaan ihmiskeholle ja joita käytetään terveyden monitorointiin, ovat digitaalisia elementtejä sisältäviä tuotteita, jotka sijoitetaan keholle suoraan tai joita pidetään yllä vaatteen tai asusteen avulla ja jotka voivat säännöllisesti tai jatkuvasti havainnoida ja käsitellä käyttäjän terveyden kannalta merkityksellisiä tietoja, mukaan lukien kehon mittaustiedot, pois lukien tuotteet, jotka kuuluvat asetuksen (EU) 2017/745 tai asetuksen (EU) 2017/746 soveltamisalaan. Tähän luokkaan kuuluvat muun muassa älyrannekkeet, -kellot, -korut, -vaatteet ja -urheiluvaatteet, jotka vastaavat tätä kuvausta.
	Lasten käyttöön ja lapsilla käytettäväksi tarkoitetut henkilökohtaiset puettavat tuotteet ovat digitaalisia elementtejä sisältäviä alle 14-vuotiaille tarkoitettuja tuotteita, jotka sijoitetaan keholle suoraan tai joita pidetään yllä vaatteen tai asusteen avulla. Tähän luokkaan kuuluvat muun muassa lapsille tarkoitetut puettavat turvalaitteet.

([1]) Euroopan parlamentin ja neuvoston direktiivi 2009/48/EY, annettu 18 päivänä kesäkuuta 2009, lelujen turvallisuudesta (EUVL L 170, 30.6.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, annettu 5 päivänä huhtikuuta 2017, lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta (EUVL L 117, 5.5.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Euroopan parlamentin ja neuvoston asetus (EU) 2017/746, annettu 5 päivänä huhtikuuta 2017, *in vitro* -diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista sekä direktiivin 98/79/EY ja komission päätöksen 2010/227/EU kumoamisesta (EUVL L 117, 5.5.2017, s. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Luokka II

Tuoteryhmä	Tekninen kuvaus
1. Virtualisointialustat ja konttien ajonaikaiset järjestelmät, jotka tukevat käyttöjärjestelmien ja vastaavien ympäristöjen virtualisoitua ajoa	Virtualisointialustat ovat digitaalisia elementtejä sisältäviä ohjelmistotuotteita, jotka abstrahoivat ja/tai jakavat laskentaresursseja ja mahdollistavat toiminnan, hallinnan ja orkestroinnin virtuaalikoneille, jotka on loogisesti erotettu toisistaan ja/tai fyysisistä laitteista. Virtualisointialustat voivat toimia suoraan laitteistolla (”bare metal”), käyttöjärjestelmän päällä tai toisessa virtuaalikoneessa (sisäkkäinen virtualisointi). Tässä tuoteryhmässä virtuaalikone on laskentaympäristöstä loogisesti erotettu ohjelmistopohjainen kokonaisuus, johon sisältyy virtuaalisia laitteistoresursseja (esimerkiksi suoritin, muisti, tallennustila, verkkorajapinnat) ja jolla on yleensä oma käyttöjärjestelmänsä. Tähän luokkaan kuuluvat muun muassa tyypin 1 virtualisointialustat (”bare metal”), (käyttöjärjestelmän päällä suoritettavat) tyypin 2 virtualisointialustat ja hybridivirtualisointialustat.
	Konttien ajonaikaiset järjestelmät ovat digitaalisia elementtejä sisältäviä ohjelmistotuotteita, jotka hallinnoivat konttien suorittamista ja elinkaarta. Ne toimivat yksittäisen isäntäkäyttöjärjestelmän päällä eristettyinä prosesseina, jakavat resursseja sekä mahdollistavat yksittäisten konttien hallinnan ja orkestroinnin. Tässä tuoteryhmässä kontti on ohjelmistopohjainen suoritusympäristö, joka kokoaa yhden tai useamman ohjelmistokomponentin ja niiden riippuvuudet yhteen pakettiin, jolloin se voi toimia itsenäisesti ja johdonmukaisesti.
2. Palomuurit ja tunkeutumisen havaitsemis- ja estojärjestelmät	Palomuurit ovat digitaalisia elementtejä sisältäviä tuotteita, jotka suojaavat kytkettyä verkkoa tai järjestelmää luvattomalta pääsyltä seuraamalla kyseisestä verkosta lähtevää ja sen ulkopuolelta tulevaa tietoliikennettä ja rajoittamalla sitä. Tähän luokkaan kuuluvat muun muassa verkon palomuurit ja sovelluspalomuurit, kuten verkkosovelluksen palomuurit tai suodattimet ja roskapostiliikenteen turvayhdyskäytävät.
	Tunkeutumisen havaitsemisjärjestelmät ovat digitaalisia elementtejä sisältäviä tuotteita, jotka seuraavat epäilyttävää liikennettä verkkoympäristössä ja havaitsevat tai tunnistavat kytketyssä verkossa tai järjestelmässä tapahtuvat tunkeutumisyritykset, meneillään olevat tunkeutumiset tai tapahtuneet tunkeutumiset. Tähän ryhmään kuuluvat muun muassa verkkopohjaiset tunkeutumisen havaitsemisjärjestelmät ja isäntäpohjaiset tunkeutumisen havaitsemisjärjestelmät.
	Tunkeutumisen estojärjestelmät ovat digitaalisia elementtejä sisältäviä tuotteita, jotka koostuvat tunkeutumisen havaitsemisjärjestelmästä, joka reagoi aktiivisesti kytketyssä verkossa tai järjestelmässä tapahtuneisiin tunkeutumisiin. Tähän ryhmään kuuluvat muun muassa verkkopohjaiset tunkeutumisen estojärjestelmät ja isäntäpohjaiset tunkeutumisen estojärjestelmät.

Tuoteryhmä	Tekninen kuvaus
3. Väärinkäytöltä suojatut mikroprosessorit	Digitaalisia elementtejä sisältävät tuotteet, jotka ovat tämän liitteen taulukossa ”Luokka I” olevassa 13 kohdassa tarkoitettuja mikroprosessoreita, joilla on turvallisuustoimintoja, mukaan lukien väärinkäytön havaitseminen, siltä suojautuminen tai siihen reagointi, ja joihin on lisäksi suunniteltu yhteisiin kriteereihin ja yhteisiin arviointimenetelmiin perustuvan AVA_VAN 2- tai 3 -tason suojaus.
4. Väärinkäytöltä suojatut mikro-ohjaimet	Digitaalisia elementtejä sisältävät tuotteet, jotka ovat tämän liitteen taulukossa ”Luokka I” olevassa 14 kohdassa tarkoitettuja mikro-ohjaimia, joilla on turvallisuustoimintoja, mukaan lukien väärinkäytön havaitseminen, siltä suojautuminen tai siihen reagointi, ja joihin on lisäksi suunniteltu yhteisten kriteerien ja yhteisten arviointimenetelmien mukainen AVA_VAN 2- tai 3 -tason suojaus.

ELI: http://data.europa.eu/eli/reg_impl/2025/2392/oj

LIITE II

DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVÄT KRIITTISET TUOTTEET

Tuoteryhmä	Tekninen kuvaus
1. Fyysiset laitteet, joissa on peukaloinnilta suojaavia turvamekanismeja	Digitaalisia elementtejä sisältävät laitteistotuotteet, jotka tallentavat, käsittelevät tai hallinnoivat arkaluonteista tietoa turvallisesti tai suorittavat salaustoimintoja. Ne koostuvat erilliskomponenteista ja fyysisestä laitekotelosta, jotka mahdollistavat peukaloinnin havaitsemisen, siltä suojautumisen tai siihen reagoinnin fyysisten hyökkäysten torjumiseksi. Tähän ryhmään kuuluvat muun muassa fyysiset maksupäätteet, laitteistoturvamoduulit, jotka generoivat ja hallinnoivat salauselementtejä, ja ajopiirturit, jotka vastaavat edellä esitettyä kuvausta.
2. Älymittareiden yhdyskäytävät Euroopan parlamentin ja neuvoston direktiivin (EU) 2019/944 ([1]) 2 artiklan 23 alakohdassa määritellyissä älykkäissä mittausjärjestelmissä ja muut kehittyneisiin turvallisuustarkoituksiin, myös kryptolaskentaan, käytettävät laitteet	Älymittareiden yhdyskäytävät ovat digitaalisia elementtejä sisältäviä tuotteita, jotka ohjaavat viestintää direktiivin (EU) 2019/944 2 artiklan 23 alakohdassa määriteltyihin älykkäisiin mittausjärjestelmiin kuuluvien tai niihin liitettyjen komponenttien ja valtuutettujen kolmansien osapuolten, kuten yleishyödyllisten palvelujen tarjoajien, välillä. Älymittareiden yhdyskäytävät keräävät, käsittelevät ja tallentavat mittaus- tai henkilötietoja, suojaavat dataa ja tietovirtoja tukemalla erityisiä salaustarpeita, kuten tietojen salausta ja salauksen purkamista, sisältävät palomuuritoimintoja ja tarjoavat keinot muiden laitteiden hallintaan. Tähän ryhmään kuuluvat muun muassa älymittareiden yhdyskäytävät, jotka liittyvät direktiivin (EU) 2019/944 2 artiklan 23 alakohdassa määriteltyihin sähköä mittaaviin älykkäisiin mittausjärjestelmiin. Ryhmään voivat myös kuulua älymittareiden yhdyskäytävät, joita käytetään muiden energialähteiden, kuten kaasun tai lämmön, kulutusta mittaavissa älykkäissä mittausjärjestelmissä, edellyttäen, että yhdyskäytävä vastaa tätä kuvausta.
3. Älykortit tai vastaavat laitteet, mukaan lukien turvaelementit	Turvaelementit ovat mikro-ohjaimia tai mikroprosessoreita, joilla on turvallisuustoimintoja, kuten väärinkäytön havaitseminen, siltä suojautuminen tai siihen reagointi. Ne yleensä tallentavat, käsittelevät tai hallinnoivat salaustoimintoja tai arkaluonteisia tietoja, kuten henkilötunnuksia tai maksutietoja. Turvaelementteihin on suunniteltu vähintään yhteisiin kriteereihin tai yhteisiin arviointimenetelmiin perustuvan AVA_VAN 4 -tason suojaus. Ne voivat olla erillistä piikomponentteja, tai ne voidaan integroida yhden sirun järjestelmiin (SoC). Turvaelementteihin voi sisältyä sovellusympäristö tai käyttöjärjestelmä, ja ne voivat sisältää yhden tai useamman sovelluksen. Tähän luokkaan kuuluvat muun muassa TPM-turvapiirit ja sulautetut UICC-kortit.
	Älykortit tai vastaavat laitteet ovat kortin muotoiseen alustamateriaaliin, esimerkiksi muoviin tai puuhun, integroituja turvaelementtejä tai muun muotoiseen alustamateriaaliin integroituja turvaelementtejä. Tähän luokkaan kuuluvat muun muassa henkilö- ja matkakortit, allekirjoitusvarmenteen sisältävät kortit, vaihdettavat UICC-kortit, fyysiset maksukortit, fyysiset kulkukortit, digitaaliset ajopiirturikortit tai maksurannekkeet, joissa on integroituja turvaelementtejä.

([1]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/944, annettu 5 päivänä kesäkuuta 2019, sähkön sisämarkkinoita koskevista yhteisistä säännöistä ja direktiivin 2012/27/EU muuttamisesta (EUVL L 158, 14.6.2019, s. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).