Euroopa Liidu
Teataja

ET
L-seeria

2025/2392

1.12.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/2392,

28. november 2025,

Euroopa Parlamendi ja nõukogu määruse (EL) 2024/2847 kohaste digielemente sisaldavate oluliste ja kriitilise tähtsusega toodete kategooriate tehnilise kirjelduse kohta

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrust (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus), ([1]) eriti selle artikli 7 lõiget 4,

ning arvestades järgmist:

(1) Määruses (EL) 2024/2847 on sätestatud digielemente sisaldavate toodete küberturvalisuse nõuded. Eelkõige on kõnealuse määruse III lisas sätestatud digielemente sisaldavate oluliste toodete kategooriad, mille suhtes kohaldatakse turule laskmisel rangemaid vastavushindamismenetlusi kui need, mida kohaldatakse muude digielemente sisaldavate toodete suhtes. Määruse (EL) 2024/2847 IV lisas on sätestatud digielemente sisaldavate kriitilise tähtsusega toodete kategooriad, mille puhul võidakse tootjatelt nõuda, et nad omandaksid Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 ([2]) kohase Euroopa küberturvalisuse sertifitseerimise kava alusel Euroopa küberturvalisuse sertifikaadi, või mille suhtes kohaldataks turule laskmisel kohustuslikku kolmanda isiku tehtavat vastavushindamist.

(2) Määruse (EL) 2024/2847 artikli 7 lõike 1 ja artikli 8 lõike 1 kohaselt määrab digielemente sisaldava toote põhifunktsioon kindlaks selle, kas digielemente sisaldav toode vastab digielemente sisaldavate oluliste või kriitilise tähtsusega toodete kategooria tehnilisele kirjeldusele ja kas selle suhtes tuleb seega kohaldada vastavushindamismenetlusi.

(3) Digielemente sisaldava toote arendamisel ja soovitud funktsioonide saavutamiseks integreerivad tootjad tavaliselt digielemente sisaldavatesse toodetesse muid komponente, mis on ka ise digielemente sisaldavad tooted ja võivad vastata oluliste või kriitilise tähtsusega toodete kategooria tehnilisele kirjeldusele. Määruse (EL) 2024/2847 kohaselt peab digielemente sisaldav toode läbima vastavushindamismenetluse, mida kohaldatakse digielemente sisaldava olulise või kriitilise tähtsusega toote suhtes juhul, kui see toode tervikuna on vastavalt kõnealuse määruse III ja IV lisale oluline või kriitilise tähtsusega toode. Näiteks sisseehitatud veebibrauseri integreerimine nutitelefonides kasutatava uudisterakenduse komponendina ei tähenda iseenesest seda, et uudisterakenduse suhtes tuleb kohaldada vastavushindamismenetlust, mida kohaldatakse digielemente sisaldavate toodete suhtes, millel on „autonoomsete ja sisseehitatud veebibrauserite“ tootekategooria põhifunktsioon. Sellegipoolest peab tootja kooskõlas määrusega (EL) 2024/2847 tagama, et digielemente sisaldav toode tervikuna vastab olulistele küberturvalisuse nõuetele. Seepärast peab tootja hindama kogu toote turvalisust, võttes vajaduse korral arvesse tootesse integreeritud komponentide või funktsioonide turvalisust. Näiteks selleks, et uudisterakenduse tootja saaks tõendada, et digielemente sisaldav toode vastab määrusele (EL) 2024/2847, peab ta tõendama, et uudisterakendus tervikuna vastab kohaldatavatele nõuetele, võttes vajaduse korral arvesse rakendusse integreeritud sisseehitatud veebibrauseri turvalisust.

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

([2]) Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Asjaolu, et digielemente sisaldav toode täidab muid käesolevas määruses sätestatud tehnilistes kirjeldustes esitatud funktsioone või neid täiendavaid funktsioone, ei tähenda iseenesest seda, et digielemente sisaldaval tootel ei ole määruse (EL) 2024/2847 III ja IV lisas sätestatud tootekategooria põhifunktsiooni. Näiteks sellised digielemente sisaldavad tooted, millel on „operatsioonisüsteemide“ tootekategooria põhifunktsioon, sisaldavad sageli selle tootekategooria tehnilises kirjelduses nimetamata lisafunktsioone täitvat tarkvara, nagu kalkulaatorid või lihtsad vektorgraafika programmid. Digielemente sisaldavad tooted sisaldavad sageli ka komponente, millel on mõne muu digielemente sisaldava olulise või kriitilise tähtsusega toote funktsioon, näiteks operatsioonisüsteem, millesse on integreeritud veebibrauseri funktsioon, või ruuter, millesse on integreeritud tulemüüri funktsioon. See ei tähenda siiski iseenesest seda, et selliste digielemente sisaldavate toodete põhifunktsioon ei ole sama mis „operatsioonisüsteemide“ või „ruuterite, internetiühenduse jaoks mõeldud modemite ja kommutaatorite“ tootekategooriatel.

(5) Seevastu sellist digielemente sisaldavat toodet, mis suudab täita määruse (EL) 2024/2847 III ja IV lisas sätestatud tootekategooria funktsioone, kuid mille põhifunktsioon ise erineb selle tootekategooria omast, ei loeta selle tootekategooria tehnilisele kirjeldusele vastavaks. Näiteks on infoturbe haldamise, automatiseerimise ja intsidentidele reageerimise tarkvara (security orchestration, automation and response – SOAR) sageli võimeline täitma „turvateabe ja -sündmuste haldamise (SIEM) süsteemide“ kategooriasse kuuluvate digielemente sisaldavate toodete funktsioone, st koguma andmeid, neid analüüsima ja esitama neid turvaeesmärkidel rakendatava teabena. Kuna aga SOARi tarkvara põhifunktsioon ei ole sama mis SIEMi süsteemil, ei käsitata seda üldjuhul vastavana „turvateabe ja -sündmuste haldamise (SIEM) süsteemide“ tootekategooria tehnilisele kirjeldusele. Samamoodi on nutitelefoni tavaliselt integreeritud komponente, mis täidavad mitme määruse (EL) 2024/2847 III ja IV lisas sätestatud tootekategooria, nagu operatsioonisüsteemi või integreeritud paroolihalduri funktsioone. Kuna aga nutitelefoni põhifunktsioon ei ole sama mis operatsioonisüsteemi või paroolihalduri põhifunktsioon, ei käsitata seda üldjuhul vastavana sellise tootekategooria tehnilisele kirjeldusele.

(6) Määruse (EL) 2024/2847 artikli 13 lõigete 2 ja 3 kohaselt peavad digielemente sisaldavate toodete tootjad rakendama määruse (EL) 2024/2847 I lisa I osas sätestatud olulisi küberturvalisuse nõudeid viisil, mis on proportsionaalne digielemente sisaldava toote riskidega, mille hindamise aluseks on digielemente sisaldava toote sihtotstarve ja mõistlikult prognoositav kasutamine ja kasutustingimused, võttes arvesse toote eeldatavat kasutusaega. Kõnealuse määruse artikli 13 lõigete 2 ja 3 kohaselt ja olenemata sellest, kas digielemente sisaldavat toodet peetakse oluliseks või kriitilise tähtsusega digielemente sisaldavaks tooteks, peavad tootjad hindama põhjalikult küberriske ja andma teada, kuidas olulisi küberturvalisuse nõudeid, kaasa arvatud testimine ja usaldusväärsuse tagamine, küberriskide hinnangus esitatud teabe põhjal rakendatakse. Kui tootja digielemente sisaldava toote põhifunktsioon vastab digielemente sisaldava olulise või kriitilise tähtsusega toote tehnilisele kirjeldusele, peab ta tõendama nõuetele vastavust, kohaldades määruse (EL) 2024/2847 artikli 32 lõigetes 2, 3, 4 või 5 kehtestatud asjakohast vastavushindamismenetlust.

(7) Käesolev määrus sisaldab näiteid digielemente sisaldavate toodete kohta, mille põhifunktsioon vastab teatavate digielemente sisaldavate oluliste või kriitilise tähtsusega toodete tehnilisele kirjeldusele. Sellised näited on üksnes kirjeldavad ega ole ammendavad.

(8) Et tagada tootjatele õiguskindlus, tuleks „muukimiskindlate mikroprotsessorite“, „muukimiskindlate mikrokontrollerite“ ning „kiipkaartide või sarnaste seadmete, sh turvaelementide“ tootekategooriatesse kuuluvaid tooteid üksteisest eristada selle alusel, kui suur on nende vastupanuvõime selliste vigade või nõrkuste võimaliku ärakasutamise suhtes, mille eest kaitsmiseks need on projekteeritud. AVA_VAN-tase on laialdaselt kasutatav ja standarditud viis sellise vastupanuvõime väljendamiseks. AVA_VAN-tasemed on kindlaks määratud avalikult kättesaadavates ühiskriteeriumide ja ühise hindamismetoodika standardites, millel põhinevad turul laialdaselt kasutusel olevad sertifitseerimisraamistikud, nagu komisjoni rakendusmäärus (EL) 2024/482 ([3]). Rakendusmäärusega

([3]) Komisjoni 31. jaanuari 2024. aasta rakendusmäärus (EL) 2024/482, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega (ELT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(EL) 2024/482 on kehtestatud Euroopa küberturvalisuse sertifitseerimise kava, mis võimaldab toodet sertifitseerida vastavalt selle usaldusväärsuse tasemele. Tuginedes ülemaailmsetele tavadele, on rakendusmäärusega (EL) 2024/482 nähtud ette võimalus anda standardite vanematel versioonidel põhinevaid sertifikaate välja kuni 2027. aasta lõpuni. Seega on määruse (EL) 2024/2847 kontekstis asjakohane lubada väljendada AVA_VAN-tasemeid nii, et viidatakse kas kõnealuste standardite viimasele versioonile või vanematele versioonidele.

(9) Käesoleva määrusega ettenähtud meetmed on kooskõlas määruse (EL) 2024/2847 artikli 62 lõike 1 kohaselt asutatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Mõisted

Käesoleva määruse kohaldamisel kasutatakse järgmisi mõisteid:

1) „ühiskriteeriumid“ – infotehnoloogia turvalisuse hindamise ühiskriteeriumid, mis on määratletud rakendusmääruse (EL) 2024/482 artikli 2 punktis 1 või kehtestatud nimetatud rakendusmääruse artikli 3 lõike 2 punktides a ja b osutatud standardites;

2) „ühine hindamismetoodika“ – infotehnoloogia turvalisuse hindamise ühine metoodika, mis on määratletud rakendusmääruse (EL) 2024/482 artikli 2 punktis 2 või kehtestatud nimetatud rakendusmääruse artikli 3 lõike 2 punktides c ja d osutatud standardites.

Artikkel 2

1. Määruse (EL) 2024/2847 III lisas loetletud I ja II klassi kuuluvate digielemente sisaldavate toodete kategooriate tehniline kirjeldus on esitatud käesoleva määruse I lisas.

2. Määruse (EL) 2024/2847 IV lisas loetletud digielemente sisaldavate toodete kategooriate tehniline kirjeldus on esitatud käesoleva määruse II lisas.

Artikkel 3

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 28. november 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

I LISA

DIGIELEMENTE SISALDAVAD OLULISED TOOTED

I klass

Tootekategooria	Tehniline kirjeldus
1. Identiteedihalduse süsteemide ja eelisjuurdepääsu haldamise tarkvara ja riistvara, sh autentimis- ja juurdepääsu kontrolli lugerid, kaasa arvatud biomeetriliste andmete lugerid	Identiteedihalduse süsteemid on digielemente sisaldavad tooted, mis pakuvad autentimise või autoriseerimise mehhanisme ning võivad pakkuda ka mehhanisme füüsiliste isikute, juriidiliste isikute, seadmete või süsteemide identiteediandmete elutsükli haldamiseks, näiteks identiteediandmete registreerimiseks, väljastamiseks, hooldamiseks ja registrist kustutamiseks. Nende süsteemide hulka kuuluvad juurdepääsu haldamise süsteemid, mis kontrollivad füüsiliste ja juriidiliste isikute ning seadmete või süsteemide juurdepääsu digitaalsetele ressurssidele või füüsilistele asukohtadele. Eelisjuurdepääsu haldamise tarkvara on juurdepääsu haldamise süsteem, mis kontrollib ja jälgib juurdepääsuõigusi organisatsiooni IT- või OT-süsteemidele ning tundlikule teabele, ning selle hulka kuuluvad süsteemid, mis rakendavad eelisõigustega kasutajate suhtes diferentseeritud juurdepääsukontrolli eeskirju. Sellesse kategooriasse kuuluvad muu hulgas autentimis- ja juurdepääsukontrolli lugerid, biomeetriliste andmete lugerid, ühekordse sisselogimise tarkvara, üksteisega seotud tarkvara kasutaja tuvastamiseks, ühekordsete paroolide tarkvara, riistvaralised autentimisseadmed, näiteks tehingu autentimise numbri (TAN) generaatorid, autentimistarkvara ja mitmikautentimise tarkvara.
2. Autonoomsed ja sisseehitatud veebibrauserid	Digielemente sisaldavad tarkvaratooted, mis võimaldavad lõppkasutajatel võrkudega (näiteks internetiga) ühendatud serverites majutatavale veebisisule ja -teenustele juurde pääseda, neid kuvada ja nendega suhelda. Tavaliselt sisaldavad need märgistuskeeles (nt HTML) kirjutatud sisu tõlgendamiseks ja kuvamiseks mõeldud brauserimootorit, veebiprotokollide (nt HTTP, HTTPS) tuge, skriptide käitamise ja kasutaja sisendi haldamise funktsionaalsust ning võimalust salvestada veebisaitidelt pärit ajutisi või püsivaid andmeid, näiteks küpsiseid. Sellesse kategooriasse kuuluvad muu hulgas brauseri funktsioone täitvad iseseisvad rakendused, teise süsteemi või rakendusega integreerimiseks ette nähtud sisseehitatud brauserid ning tehisintellekti agendiga integreeritud brauserid.
3. Paroolihaldurid	Digielemente sisaldavad tooted, mis salvestavad paroole kas kohapeal seadmes või kaugserveris ning viivad ellu selliseid toiminguid nagu paroolide genereerimine ning paroolide jagamine ja paroolide kasutamiseks kohalike või kolmandate isikute rakendustega integreerimine. See kategooria hõlmab muu hulgas kohalikke paroolihaldureid, veebibrauseri laiendustena pakutavaid paroolihaldureid, ettevõtetele mõeldud paroolihaldureid ning riistvarapõhiseid paroolihaldureid.

Tootekategooria	Tehniline kirjeldus
4. Tarkvara, mis otsib pahavara, kõrvaldab selle või paneb karantiini	Digielemente sisaldavad tarkvaratooted, mida tavaliselt nimetatakse viirusetõrje- või kahjurvara tõrje tarkvaraks ja mis tuvastavad või otsivad seadmetes pahavara või pahatahtlikku koodi või kõrvaldavad või panevad sellise tarkvara või koodi karantiini, et tagada nende seadmete terviklus, konfidentsiaalsus ja käideldavus. Käesoleva tootekategooria kontekstis tähendab pahavara tarkvara, mis sisaldab pahatahtlikke funktsioone või võimeid, mis võivad otseselt või kaudselt kahjustada kasutajat ja/või arvutisüsteemi, näiteks viirused, arvutiussid, lunavara, nuhkvara ja troojalased. See tootekategooria hõlmab muu hulgas tarkvara, mis tuvastab või otsib pahavara reaalajas või käsitsi, juurkrattide tuvastamise tarkvara ning päästeplaate, mille põhifunktsiooniks on pahavara otsimine, kõrvaldamine või karantiini panemine.
5. Digielemente sisaldavad tooted, millel on virtuaalse privaatvõrgu (VPN) funktsioon	Digielemente sisaldavad tooted, mis loovad füüsilise või virtuaalse võrgu süsteemiressursside põhjal moodustatud krüptitud loogilise tunneli. See kategooria hõlmab muu hulgas virtuaalse privaatvõrgu kliente, virtuaalse privaatvõrgu servereid ja virtuaalse privaatvõrgu võrgulüüse.
6. Võrguhalduse süsteemid	Digielemente sisaldavad tooted, mis haldavad ühendatud võrguelemente, näiteks servereid, ruutereid, kommutaatoreid, tööjaamu, printereid või mobiilseadmeid, jälgides neid ning juhtides nende võrgutoiminguid ja konfigureerimist. Sellesse kategooriasse kuuluvad muu hulgas terviklikud haldussüsteemid ja spetsiaalsed konfiguratsioonihaldussüsteemid, näiteks tarkvarapõhise võrgustamise kontrollerid.
7. Turvateabe ja -sündmuste haldamise (SIEM) süsteemid	Digielemente sisaldavad tooted, mis koguvad andmeid mitmest allikast, analüüsivad ja korreleerivad neid ning esitavad need turvalisusega seotud eesmärkidel kasutatava teabena, näiteks ohtude ja intsidentide tuvastamiseks, kohtueksperti isi analüüsiks või nõuetele vastavuse tagamiseks.
8. Buutimishaldurid	Digielemente sisaldavad tarkvaratooted, mis haldavad süsteemi esmase käivitamise protsessi pärast sisselülitamist või taaskäivitamist, lähtestades riistvara, laadides operatsioonisüsteemi või andes juhtimise üle operatsioonisüsteemi keskkonnale või süsteemiressurssidele ning valides alglaadimise valikuid. Sellesse kategooriasse kuuluvad muu hulgas UEFI püsivara ning ühe- ja mitmeastmelised alglaadurid.
9. Avaliku võtme taristu ja digisertifikaatide väljaandmise tarkvara	Digielemente sisaldavad tooted, mida kasutatakse avaliku võtme taristu osana ning mis haldavad digisertifikaatide valideerimist, loomist, väljaandmist, levitamist, oleku avaldamist, uuendamist või tühistamist või mis haldavad selliste digisertifikaatidega seotud krüptovõtmete genereerimist, salvestamist, hoiustust, vahetamist, hävitamist või võtmete roteerimist. Sellesse kategooriasse kuuluvad muu hulgas võtmehaldussüsteemid, digisertifikaatide haldussüsteemid, OCSP (Online Certificate Status Protocol) kehtivuskinnitused ning integreeritud avaliku võtme taristu lahendused.

Tootekategooria	Tehniline kirjeldus
10. Füüsilised ja virtuaalsed võrguliidesed	Füüsilised võrguliidesed on digielemente sisaldavad tooted, mis ühendavad seadme otse võrguga liidese draiverite pakutava rakendusliidese (API) kaudu, töötades tavaliselt lülikihis, ning mis sisaldavad riistvaralisi adaptereid edastuskanalite jaoks koos vastava püsivaraga, mis töötab tavaliselt füüsilises ja lülikihis. Virtuaalsed võrguliidesed on digielemente sisaldavad tooted, mis ühendavad seadme otse või kaudselt võrguga rakendusliidese (API) kaudu, mis emuleerib füüsiliste võrguliideste draiverite rakendusliidest ja töötab tavaliselt lülikihis. Sellesse kategooriasse kuuluvad muu hulgas traadiga ja traadita võrgukaardid, kontrollerid ja adapterid, näiteks WiFi, Etherneti, IrDA, USB, Bluetoothi, NearLinki, Zigbee või Fieldbusi jaoks, samuti puhtalt virtuaalsed iseseisvad tooted, näiteks virtuaalsed võrgukaardid, konteineri võrguliidesed ja VPN-liidesed.
11. Operatsioonisüsteemid	Digielemente sisaldavad tarkvaratooted, mis pakuvad alusriistvara abstraktset liidest ja kontrollivad tarkvara käitamist ning võivad pakkuda teenuseid, nagu arvutusressursside haldamine ja konfigureerimine, ajastamine, sisend-väljundjuhtimine, andmete haldamine ja liidese pakkumine, mille kaudu rakendused suhtlevad süsteemiressursside ja välisseadmetega. Sellesse kategooriasse kuuluvad muu hulgas reaalajaoperatsioonisüsteemid ning üld- ja eriotstarbelised operatsioonisüsteemid.
12. Ruuterid, internetiühenduse jaoks mõeldud modemid ja kommutaatorid	Ruuterid on digielemente sisaldavad tooted, mis loovad ja juhivad andmevoogu eri võrkude vahel, valides marsruutimisprotokollide mehhanismide ja algoritmide abil teekondi või marsruute ning mis töötavad tavaliselt võrgukihis. See kategooria hõlmab muu hulgas traadiga ja traadita ruutereid, virtuaalseid ruutereid ning ruutereid koos modemiga või ilma selleta.
	Internetiühenduse jaoks mõeldud modemid on digielemente sisaldavad riistvaratooted, mis kasutavad digitaalset modulatsiooni- ja demodulatsioonitehnikat analoogsignaalide teisendamiseks digitaalseteks signaalideks ja vastupidi IP-põhise side jaoks. See kategooria hõlmab muu hulgas fiiberoptilisi modemeid, digitaalse abonendiliini (DSL) modemeid, kaabelmodemeid (DOCSIS), satelliitmodemeid ja mobiilside modemeid.
	Kommutaatorid on digielemente sisaldavad tooted, mis tagavad ühenduvuse võrku ühendatud seadmete vahel pakettide edastamise mehhanismide kaudu ning millel on haldustasand, mis on tavaliselt rakendatud lüli- või võrgukihis. See kategooria hõlmab muu hulgas hallatavaid kommutaatoreid, tarku kommutaatoreid, mitmekihilisi kommutaatoreid, virtuaalseid turvakommutaatoreid, tarkvarapõhise võrgustamise jaoks programmeeritavaid kommutaatoreid ning sildu, näiteks traadita pääsupunkte.

Tootekategooria	Tehniline kirjeldus
13. Turvafunktsioonidega mikroprotsessorid	Digielemente sisaldavad tooted, mille puhul on tegemist keskse töötlemise funktsioone täitvate integraallülitustega, mis tuginevad välismälule ja välisseadmetele, sealhulgas mikrokoodile ja muule madaltaseme püsivarale. Lisaks pakuvad need turvafunktsioone, näiteks krüpteerimist, autentimist, turvalist võtmetalletust, juhuarvude genereerimist, usaldatavat täitmiskeskkonda või muid riistvarapõhiseid kaitsemehhanisme, mille eesmärk on turvata lisaks mikroprotsessorile endale ka teisi tooteid, võrke või teenuseid, milleks on näiteks turvaline alglaadimisahel, virtualiseerimine või turvalised sideliidesed.
14. Turvafunktsioonidega mikrokontrollerid	Digielemente sisaldavad tooted, mille puhul on tegemist mälu integreerivate keskse töötlemise funktsioone täitvate integraallülitustega, mis võimaldavad programmeerida mikrokontrollerit ning tavaliselt ka muid välisseadmeid, sealhulgas mikrokoodi ja muud madaltaseme püsivara. Lisaks pakuvad need turvafunktsioone, näiteks krüpteerimist, autentimist, turvalist võtmetalletust, juhuarvude genereerimist, usaldatavat täitmiskeskkonda või muid riistvarapõhiseid kaitsemehhanisme, mille eesmärk on turvata lisaks mikrokontrollerile endale ka teisi tooteid, võrke või teenuseid, milleks on näiteks turvaline alglaadimise ahel, virtualiseerimine või turvalised sideliidesed.
15. Turvafunktsioonidega rakendusspetsiifilised integraallülitused (ASIC) ja programmeeritavad ventiilimaatriksid (FPGA)	Turvafunktsioonidega rakendusspetsiifilised integraallülitused (ASIC) on digielemente sisaldavad tooted; tegemist on integraallülitustega, mis on täielikult või osaliselt kohandatud konkreetse funktsiooni täitmiseks või konkreetse rakenduse rakendamiseks, sh mikrokood ja muu madaltaseme püsivara. Lisaks pakuvad need turvafunktsioone, näiteks krüpteerimist, autentimist, turvalist võtmetalletust, juhuarvude genereerimist, usaldatavat täitmiskeskkonda või muid riistvarapõhiseid kaitsemehhanisme, mille eesmärk on turvata lisaks turvafunktsioonidega rakendusspetsiifilisele integraallülitusele endale ka teisi tooteid, võrke või teenuseid, milleks on näiteks turvaline alglaadimise ahel, virtualiseerimine või turvalised sideliidesed.
	Turvafunktsioonidega programmeeritavad ventiilimaatriksid (FPGA) on digielemente sisaldavad tooted; tegemist on integraallülitustega, mida iseloomustab konfigureeritavate loogikaplokkide maatriks, mis on projekteeritud selliselt, et seda saab pärast tootmist ümber programmeerida konkreetse funktsiooni täitmiseks või konkreetse rakenduse rakendamiseks, sh mikrokood ja muu madaltaseme püsivara. Lisaks pakuvad need turvafunktsioone, näiteks krüpteerimist, autentimist, turvalist võtmetalletust, juhuarvude genereerimist, usaldatavat täitmiskeskkonda või muid riistvarapõhiseid kaitsemehhanisme, mille eesmärk on turvata lisaks programmeeritavale ventiilimaatriksile endale ka teisi tooteid, võrke või teenuseid, milleks on näiteks turvaline alglaadimise ahel, virtualiseerimine või turvalised sideliidesed.
16. Nutikodu üldotstarbelised virtuaalassistendid	Digielemente sisaldavad tooted, mis suhtlevad avalikus internetis kas otse või muu seadme vahendusel, mis töötlevad loomulikus keeles esitatud korraldusi, ülesandeid või küsimusi, näiteks heli- või kirjaliku sisendi kaudu, ning mis nende korralduste, ülesannete või küsimuste alusel võimaldavad juurdepääsu muudele teenustele või juhivad eluruumides kasutatavate ühendatud seadmete funktsioone. Sellesse kategooriasse kuuluvad muu hulgas integreeritud virtuaalassistendiga nutikõlarid ning käesolevale kirjeldusele vastavad eraldiseisvad virtuaalassistendid.

Tootekategooria	Tehniline kirjeldus
17. Turvafunktsioonidega nutikodu tooted, sh arukad ukselukud, turvakaamerad, beebimonitorisüsteemid ja häiresüsteemid	Digielemente sisaldavad tooted, mis kaitsevad tarbijate füüsilist turvalisust eluruumides ja mida saab teistest süsteemidest kaugjuhtimise teel või kaugelt hallata, samuti selliseid tooteid tsentraalselt juhtiv riistvara ja tarkvara. Sellesse kategooriasse kuuluvad muu hulgas nutilukud, imikumonitorid, häiresüsteemid ja koduvalvekaamerad.
18. Euroopa Parlamendi ja nõukogu direktiiviga 2009/48/EÜ ([1]) hõlmatud internetiühendusega mänguasjad, millel on interaktiivsed sotsiaalfunktsioonid (nt rääkimine või filmimine) või asukoha jälgimise funktsioonid	Internetiühendusega mänguasjad, millel on interaktiivsed sotsiaalfunktsioonid, on direktiivi 2009/48/EÜ kohaldamisalasse kuuluvad digielemente sisaldavad tooted, mis suhtlevad avalikus internetis kas otse või muu seadme vahendusel ning millel on sisseehitatud tehnoloogia, mis võimaldab sissetulevat ja väljaminevat sidet, näiteks klaviatuuri, mikrofoni, valjuhääldi või kaamera kaudu.
	Internetiühendusega mänguasjad, millel on asukoha jälgimise funktsioonid, on direktiivi 2009/48/EÜ kohaldamisalasse kuuluvad digielemente sisaldavad tooted, mis suhtlevad avalikus internetis kas otse või muu seadme vahendusel ning millel on tehnoloogiad, mis võimaldavad mänguasja või selle kasutaja geograafilise asukoha jälgimist või tuletamist. Kui mänguasi tuvastab andurite abil üksnes kasutaja või muude mänguasjade lähedust, ei loeta seda asukoha jälgimise funktsiooniga mänguasjaks.
19. Inimkehal kantavad või inimkehale paigutatavad isiklikud kantavad tooted, millel on terviseseire (nt jälgimise) eesmärk ja mille suhtes ei kohaldata Euroopa Parlamendi ja nõukogu määrust (EL) 2017/745 ([2]) ega määrust (EL) 2017/746, ([3]) või isiklikud kantavad tooted, mis on ette nähtud kasutamiseks laste poolt ja lastel	Inimkehal kantavad või inimkehale paigutatavad isiklikud kantavad tooted, millel on terviseseire (nt jälgimise) eesmärk, on digielemente sisaldavad tooted, mida kantakse kehal vahetult või riiete või tarvikute kaudu ning mis suudavad regulaarselt või pidevalt tuvastada ja edasi töödelda kasutaja tervisega seotud teavet, sh kehaparameetreid; siia ei kuulu tooted, mille suhtes kohaldatakse määrust (EL) 2017/745 või määrust (EL) 2017/746. Sellesse kategooriasse kuuluvad muu hulgas aktiivsusmonitorid, nutikellad, -ehted, -riided ja -spordirõivad, mis vastavad käesolevale kirjeldusele.
	Laste poolt ja lastel kasutamiseks ette nähtud isiklikud kantavad tooted on digielemente sisaldavad tooted, mida alla 14aastased isikud saavad kanda inimkehal või inimkehale paigutada vahetult või riiete või tarvikute kaudu. Sellesse kategooriasse kuuluvad muu hulgas laste turvalisust tagavad kantavad seadmed.

([1]) Euroopa Parlamendi ja nõukogu 18. juuni 2009. aasta direktiiv 2009/48/EÜ mänguasjade ohutuse kohta (ELT L 170, 30.6.2009, lk 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/745, milles käsitletakse meditsiiniseadmeid, millega muudetakse direktiivi 2001/83/EÜ, määrust (EÜ) nr 178/2002 ja määrust (EÜ) nr 1223/2009 ning millega tunnistatakse kehtetuks nõukogu direktiivid 90/385/EMÜ ja 93/42/EMÜ (ELT L 117, 5.5.2017, lk 1, ELI: http://data.europa.eu/eli/reg/2017/745/et).

([3]) Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/746 *in vitro* diagnostikameditsiiniseadmete kohta ning millega tunnistatakse kehtetuks direktiiv 98/79/EÜ ja komisjoni otsus 2010/227/EL (ELT L 117, 5.5.2017, lk 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

II klass

Tootekategooria	Tehniline kirjeldus
1. Hüperviisorid ja konteinerite käigusüsteemid, mis toetavad operatsioonisüsteemide ja samalaadsete keskkondade virtualiseeritud käitamist	Hüperviisorid on digielemente sisaldavad tarkvaratooted, mis abstraheerivad ja/või jaotavad arvutusressursse ning võimaldavad üksteisest ja/või füüsilisest riistvarast loogiliselt eraldatud virtuaalmasinate käitamist, haldamist ja orkestreerimist. Hüperviisorid võivad töötada otse riistvaral (*bare metal*), operatsioonisüsteemil või teise virtuaalmasina sees (pesastatud virtualiseerimine). Käesoleva tootekategooria kontekstis on virtuaalmasin tarkvarapõhine arvutuskeskkonna loogiline eraldus, mis hõlmab virtuaalsete riistvararessursside kogumit (näiteks protsessor, mälu, andmesalvesti, võrguliidesed) ja mis käitab tavaliselt oma operatsioonisüsteemi. Sellese kategooriasse kuuluvad muu hulgas 1. tüübi hüperviisorid (riistvaral töötavad), 2. tüübi hüperviisorid (operatsioonisüsteemil töötavad) ning hübriidhüperviisorid.
	Konteinerite käigusüsteemid on digielemente sisaldavad tarkvaratooted, mis haldavad ühel *host*-operatsioonisüsteemil eraldatud protsessidena töötavate konteinerite käitamist ja elutsüklit, jaotades ressursse ning võimaldades üksikute konteinerite haldamist ja orkestreerimist. Käesoleva tootekategooria kontekstis on konteiner tarkvarapõhine täitmiskeskkond, mis kapseldab ühte või mitut tarkvarakomponenti ja nende sõltuvusi ühte paketti, võimaldades selle ühtset ja sõltumatut käitamist.
2. Tulemüürid, sissetungi tuvastamise ja ennetamise süsteemid	Tulemüürid on digielemente sisaldavad tooted, mis kaitsevad ühendatud võrku või süsteemi loata juurdepääsu eest, jälgides ja piirates sellesse võrku suunduvat ja sellest võrgust lähtuvat andmesideliiklust. Sellesse kategooriasse kuuluvad muu hulgas võrkude ja rakenduste tulemüürid, näiteks veebirakenduste tulemüürid või filtrid ja rämpsposti tõkestamise lüüsid.
	Sissetungi tuvastamise süsteemid on digielemente sisaldavad tooted, mis jälgivad võrgukeskkonda juba sisenenud liiklust kahtlase tegevuse suhtes ning mille abil avastatakse või tuvastatakse, et ühendatud võrku või süsteemi on üritatud, parajasti üritatakse või on juba õnnestunud sisse tungida. Sellesse kategooriasse kuuluvad muu hulgas võrgupõhised sissetungi tuvastamise süsteemid ja hostipõhised sissetungi tuvastamise süsteemid.
	Sissetungi ennetamise süsteemid on digielemente sisaldavad tooted, mis koosnevad sissetungi tuvastamise süsteemist, mis reageerib aktiivselt sissetungile, mis toimub ühendatud võrku või süsteemi. Sellesse kategooriasse kuuluvad muu hulgas võrgupõhised sissetungi ennetamise süsteemid ja hostipõhised sissetungi ennetamise süsteemid.

Tootekategooria	Tehniline kirjeldus
3. Muukimiskindlad mikroprotsessorid	Digielemente sisaldavad tooted, mis on käesoleva lisa tabeli „I klass“ punktis 13 nimetatud turvafunktsioonidega mikroprotsessorid, mis hõlmavad muukimise tõendamise või takistamise või muukimisele reageerimise funktsioone ning mis lisaks on kavandatud tagama kaitse tasemel AVA_VAN.2 või AVA_VAN.3 vastavalt ühiskriteeriumidele ja ühisele hindamismetoodikale.
4. Muukimiskindlad mikrokontrollerid	Digielemente sisaldavad tooted, mis on käesoleva lisa tabeli „I klass“ punktis 14 nimetatud turvafunktsioonidega mikrokontrollerid, mis hõlmavad muukimise tõendamise või takistamise või muukimisele reageerimise funktsioone ning mis lisaks on kavandatud tagama kaitse tasemel AVA_VAN.2 või AVA_VAN.3 vastavalt ühiskriteeriumidele ja ühisele hindamismetoodikale.

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

II LISA

DIGIELEMENTE SISALDAVAD KRIITILISE TÄHTSUSEGA TOOTED

Tootekategooria	Tehniline kirjeldus
1. Turvalaegastega riistvaraseadmed	Digielemente sisaldavad riistvaratooted, mis talletavad, töötlevad või haldavad turvaliselt tundlikke andmeid või teostavad krüptotoiminguid ning mis koosnevad mitmest diskreetsest komponendist, hõlmates riistvara füüsilist ümbrist, mis pakub füüsiliste rünnete vastumeetmetena muukimise tõendamist või takistamist või muukimisele reageerimist. Sellesse kategooriasse kuuluvad muu hulgas füüsilised makseterminalid, krüptoelemente genereerivad ja haldavad riistvaralised turvamoodulid ning käesolevale kirjeldusele vastavad sõidumeerikud.
2. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/944 ([1]) artikli 2 punktis 23 määratletud nutiarvestisüsteemide nutiarvestite lüüsid ja muud seadmed kõrgema turvalisuse tagamiseks, sh turvaliseks krüptotöötluseks	Nutiarvesti lüüsid on digielemente sisaldavad tooted, mis juhivad suhtlust direktiivi (EL) 2019/944 artikli 2 punktis 23 määratletud nutiarvestisüsteemi koosseisu kuuluvate või nendega ühendatud komponentide ja volitatud kolmandate isikute, näiteks energiaettevõtjate vahel. Nutiarvesti lüüsid koguvad, töötlevad ja talletavad arvesti- või isikuandmeid, kaitsevad andmeid ja teabevooge, toetades spetsiifilisi krüpteerimisvajadusi, näiteks andmete krüpteerimist ja dekrüpteerimist, sisaldavad tulemüürifunktsioone ning võimaldavad teiste seadmete juhtimist. Sellesse kategooriasse kuuluvad muu hulgas nutiarvesti lüüsid, mis on seotud elektrienergiat mõõtvate nutiarvestisüsteemidega, nagu on määratletud direktiivi (EL) 2019/944 artikli 2 punktis 23. See võib hõlmata ka teistes nutiarvestisüsteemides kasutatavaid nutiarvesti lüüse, mis mõõdavad muu energiaallika, näiteks gaasi või soojuse tarbimist, tingimusel et lüüs vastab käesolevale kirjeldusele.
3. Kiipkaardid või sarnased seadmed, sh turvaelemendid	Turvaelemendid on mikrokontrollerid või mikroprotsessorid, millel on turvafunktsioonid, sealhulgas muukimise tõendamist või takistamist või muukimisele reageerimist võimaldavad funktsioonid. Need salvestavad, töötlevad või haldavad tavaliselt krüptotoiminguid või tundlikke andmeid, näiteks identiteedi- või makseandmeid. Turvaelemendid on kavandatud tagama kaitse vähemalt tasemel AVA_VAN.4, nagu on sätestatud ühiskriteeriumides või ühises hindamismetoodikas. Need võivad olla eraldi ränikiibid või integreeritud kiibisüsteemidesse (system-on-chip – SoC; monokiipsüsteem). Turvaelemendid võivad hõlmata rakenduskeskkonda või operatsioonisüsteemi ning sisaldada ühte või mitut rakendust. Sellesse kategooriasse kuuluvad muu hulgas usaldatavad platvormimoodulid (Trusted Platform Modules – TPM) ja universaalsed kiipkaardid (Universal Integrated Circuit Card – UICC).
	Kiipkaardid või sarnased seadmed on kaardikujulised turvaelemendid, mis on integreeritud kandematerjali, näiteks plasti või puidu sisse, või muukujulised turvaelemendid, mis on integreeritud muusse kandematerjali. Sellesse kategooriasse kuuluvad muu hulgas isiku- ja reisidokumendid, kvalifitseeritud allkirjakaardid, vahetatavad UICC-d, füüsilised maksekaardid, füüsilised juurdepääsukaardid, digitaalsed sõidumeerikukaardid või integreeritud makseturvaelemendiga käevõrud.

([1]) Euroopa Parlamendi ja nõukogu 5. juuni 2019. aasta direktiiv (EL) 2019/944 elektrienergia siseturu ühiste normide kohta ja millega muudetakse direktiivi 2012/27/EL (ELT L 158, 14.6.2019, lk 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).