Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/2392

1.12.2025.

# KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/2392

**(2025. gada 28. novembris)**

**par nozīmīgu un kritiski svarīgu produktu ar digitāliem elementiem kategoriju tehnisko aprakstu saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2024/2847**

**(Dokuments attiecas uz EEZ)**

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2024/2847 (2024. gada 23. oktobris) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulas (ES) Nr. 168/2013 un (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts) ([1]), un it īpaši tās 7. panta 4. punktu,

tā kā:

(1) Regulā (ES) 2024/2847 ir paredzētas kiberdrošības prasības attiecībā uz produktiem ar digitāliem elementiem. Konkrētāk, minētās regulas III pielikumā ir noteiktas tādu nozīmīgu produktu ar digitāliem elementiem kategorijas, uz kuriem, tos laižot tirgū, attiecas stingrākas atbilstības novērtēšanas procedūras nekā tās procedūras, ko piemēro citiem produktiem ar digitāliem elementiem. Regulas (ES) 2024/2847 IV pielikumā ir noteiktas kritiski svarīgu produktu ar digitāliem elementiem kategorijas, attiecībā uz kurām ražotājiem varētu prasīt saņemt Eiropas kiberdrošības sertifikātu saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu atbilstoši Eiropas Parlamenta un Padomes Regulai (ES) 2019/881 ([2]) vai uz kurām, laižot tirgū, attiektos obligāts trešās personas atbilstības novērtējums.

(2) Saskaņā ar Regulas (ES) 2024/2847 7. panta 1. punktu un 8. panta 1. punktu produkta ar digitāliem elementiem pamatfunkcionalitāte nosaka, vai minētais produkts ar digitāliem elementiem atbilst nozīmīgu vai kritiski svarīgu produktu ar digitāliem elementiem kategorijas tehniskajam aprakstam un līdz ar to piemērojamajām atbilstības novērtēšanas procedūrām.

(3) Izstrādājot produktu ar digitāliem elementiem un lai panāktu vēlamo funkciju kopumu, ražotāji savos produktos ar digitāliem elementiem parasti integrē citus komponentus, kas arī ir produkti ar digitāliem elementiem un kas var atbilst nozīmīgu vai kritiski svarīgu produktu kategorijas tehniskajam aprakstam. Saskaņā ar Regulu (ES) 2024/2847 uz produktu ar digitāliem elementiem attiecas atbilstības novērtēšanas procedūras, kas piemērojamas nozīmīgiem vai kritiski svarīgiem produktiem ar digitāliem elementiem, ja minētais produkts kopumā ir nozīmīgs vai kritiski svarīgs produkts, kā noteikts minētās regulas III un IV pielikumā. Piemēram, iegultās pārlūkprogrammas kā viedtālruņos lietojamas ziņu lietotnes komponenta integrēšana pati par sevi nenozīmē, ka uz ziņu lietotni attiecas atbilstības novērtēšanas procedūra, kas piemērojama produktiem ar digitāliem elementiem, kuru pamatfunkcija ir "atsevišķas un iegultas pārlūkprogrammas". Tomēr saskaņā ar Regulu (ES) 2024/2847 ražotājam ir jānodrošina, ka produkts ar digitāliem elementiem kopumā atbilst kiberdrošības pamatprasībām. Tāpēc ražotājam ir jānovērtē visa produkta drošība, attiecīgā gadījumā ņemot vērā tajā integrēto komponentu vai funkciju drošību. Piemēram, lai ziņu lietotnes ražotājs varētu pierādīt, ka tā produkts ar digitāliem elementiem atbilst Regulai (ES) 2024/2847, šim ražotājam ir jāpierāda, ka ziņu lietotne kopumā atbilst piemērojamajām prasībām, attiecīgā gadījumā ņemot vērā tā lietotnē integrētās iegultās pārlūkprogrammas drošību.

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

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Tas, ka produkts ar digitāliem elementiem veic funkcijas, kas nav funkcijas, kuras sīki izklāstītas šajā regulā norādītajos tehniskajos aprakstos, vai kas ir papildu funkcijas, pats par sevi nenozīmē, ka produktam ar digitāliem elementiem nav Regulas (ES) 2024/2847 III un IV pielikumā noteiktās produktu kategorijas pamatfunkciju. Piemēram, produkti ar digitāliem elementiem, kuriem ir "operētājsistēmu" pamatfunkcija, bieži ietver programmatūru, kas veic palīgfunkcijas, kuras nav iekļautas minētās produktu kategorijas tehniskajā aprakstā, piemēram, kalkulatori vai vienkārši grafiskie redaktori. Produkti ar digitāliem elementiem bieži ietver arī komponentus, kuriem ir cita nozīmīga vai kritiski svarīga produkta ar digitāliem elementiem funkcija, piemēram, operētājsistēma, kas integrē pārlūkprogrammas funkciju, vai maršrutētājs, kas integrē ugunsmūra funkciju. Tomēr tas pats par sevi nenozīmē, ka šādiem produktiem ar digitāliem elementiem nav attiecīgi "operētājsistēmu" vai "maršrutētāju, modemu, kas paredzēti savienojumam ar internetu, un komutatoru" pamatfunkciju.

(5) No otras puses, produkts ar digitāliem elementiem, kas spēj veikt Regulas (ES) 2024/2847 III un IV pielikumā noteiktas produktu kategorijas funkcijas, bet kura pamatfunkcija pati par sevi atšķiras no šādas produktu kategorijas funkcijas, nav uzskatāms par atbilstošu minētās produktu kategorijas tehniskajam aprakstam. Piemēram, drošības orķestrācijas, automatizācijas un reaģēšanas (*SOAR*) programmatūra bieži spēj veikt produktu ar digitāliem elementiem funkcijas kategorijā "drošības informācijas un notikumu pārvaldības (*SIEM*) sistēmas", t. i., vākt, analizēt un norādīt datus kā drošības nolūkos izmantojamu informāciju. Tomēr, tā kā *SOAR* programmatūras pamatfunkcija nav *SIEM* funkcija, parasti uzskata, ka tā neatbilst "drošības informācijas un notikumu pārvaldības (*SIEM*) sistēmu" tehniskajam aprakstam. Tāpat viedtālrunī parasti ir integrēti komponenti, kas veic vairāku Regulas (ES) 2024/2847 III un IV pielikumā noteikto produktu kategoriju funkcijas, piemēram, operētājsistēma vai integrēts paroļu pārvaldnieks. Tomēr, tā kā viedtālruņa pamatfunkcija nav operētājsistēmas vai paroļu pārvaldīšanas funkcija, to parasti neuzskata par atbilstošu šādu produktu kategoriju tehniskajam aprakstam.

(6) Saskaņā ar Regulas (ES) 2024/2847 13. panta 2. un 3. punktu produktu ar digitāliem elementiem ražotājiem Regulas (ES) 2024/2847 I pielikuma I daļā noteiktās kiberdrošības pamatprasības jāīsteno samērīgi ar produkta ar digitāliem elementiem riskiem, pamatojoties uz paredzēto nolūku un pamatoti paredzamo lietojumu, kā arī produkta ar digitāliem elementiem lietošanas nosacījumiem, ņemot vērā paredzamo produkta lietošanas ilgumu. Saskaņā ar minētās regulas 13. panta 2. un 3. punktu un neatkarīgi no tā, vai produkts ar digitāliem elementiem tiek uzskatīts par nozīmīgu vai kritiski svarīgu produktu ar digitāliem elementiem, ražotājiem ir jāveic visaptverošs kiberdrošības riska novērtējums un jānorāda, kā tiek īstenotas kiberdrošības pamatprasības, pamatojoties uz riska novērtējumu, tostarp to testēšana un apliecināšana. Ja produkta ar digitāliem elementiem pamatfunkcionalitāte atbilst nozīmīga vai kritiski svarīga produkta ar digitāliem elementiem tehniskajam aprakstam, ražotājiem ir jāpierāda atbilstība, ievērojot īpašās atbilstības novērtēšanas procedūras, kas noteiktas ar Regulas (ES) 2024/2847 32. panta 2., 3., 4. un 5. punktu.

(7) Šajā regulā ir iekļauti tādu produktu ar digitāliem elementiem piemēri, kuru pamatfunkcija atbilst dažu nozīmīgu vai kritiski svarīgu produktu ar digitāliem elementiem tehniskajam aprakstam. Šādi piemēri ir sniegti tikai ilustratīviem mērķiem un nav izsmeļošs saraksts.

(8) Lai ražotājiem nodrošinātu juridisko noteiktību, tādu produktu ar digitāliem elementiem kategorijas, kas ir pret iejaukšanos droši mikroprocesori, pret iejaukšanos droši mikrokontrolleri, viedkartes un līdzīgas ierīces, tostarp drošības elementi, būtu jānošķir, pamatojoties uz to, cik lielā mērā šie produkti ir noturīgi pret to trūkumu vai nepilnību iespējamu izmantošanu, kurām tie ir izstrādāti. AVA_VAN līmenis ir plaši izmantots un standartizēts veids, kā izteikt šādu noturības līmeni. AVA_VAN līmeņi ir noteikti publiski pieejamajos vienotajos kritērijos un vienotās izvērtēšanas metodikas standartos, kas ir pamatā esošajiem sertifikācijas satvariem, kuri tiek plaši pieņemti tirgū, piemēram, Komisijas Īstenošanas regulā (ES) 2024/482 ([3]). Ar Īstenošanas regulu (ES) 2024/482 ir izveidota

([3]) Komisijas Īstenošanas regula (ES) 2024/482 (2024. gada 31. janvāris) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (OV L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

Eiropas kiberdrošības sertifikācijas shēma, ko var izmantot produkta sertificēšanai noteiktā apliecinājuma līmenī. Pamatojoties uz globālo praksi, Īstenošanas regula (ES) 2024/482 paredz iespēju līdz 2027. gada beigām izdot sertifikātus, kas balstīti uz vecākām standartu versijām. Tādējādi Regulas (ES) 2024/2847 kontekstā ir lietderīgi ļaut AVA_VAN līmeņus izteikt, atsaucoties vai nu uz jaunāko, vai arī uz vecākām šo standartu versijām.

(9) Šajā regulā paredzētie pasākumi ir saskaņā ar atzinumu, kuru sniegusi komiteja, kas izveidota saskaņā ar Regulas (ES) 2024/2847 62. panta 1. punktu,

IR PIEŅĒMUSI ŠO REGULU.

*1. pants*

**Definīcijas**

Šajā regulā izmanto šādas definīcijas:

1) "vienotie kritēriji" ir vienotie informācijas tehnoloģiju drošības izvērtēšanas kritēriji, kā definēts Īstenošanas regulas (ES) 2024/482 2. panta 1. punktā vai noteikts minētās īstenošanas regulas 3. panta 2. punkta a) un b) apakšpunktā minētajos standartos;

2) "vienotā izvērtēšanas metodika" ir vienotā informācijas tehnoloģiju drošības izvērtēšanas metodika, kā definēts Īstenošanas regulas (ES) 2024/482 2. panta 2. punktā vai noteikts minētās īstenošanas regulas 3. panta 2. punkta c) un d) apakšpunktā minētajos standartos.

*2. pants*

1. Regulas (ES) 2024/2847 III pielikumā uzskaitīto I un II klases produktu ar digitāliem elementiem kategoriju tehnisko aprakstu izklāsta šīs regulas I pielikumā.

2. Regulas (ES) 2024/2847 IV pielikumā uzskaitīto produktu ar digitāliem elementiem kategoriju tehnisko aprakstu izklāsta šīs regulas II pielikumā.

*3. pants*

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2025. gada 28. novembrī

*Komisijas vārdā –*
*priekšsēdētāja*
Ursula VON DER LEYEN

*I PIELIKUMS*

**NOZĪMĪGI PRODUKTI AR DIGITĀLIEM ELEMENTIEM**

**I klase**

| Produkta kategorija | Tehniskais apraksts |
|---|---|
| 1. Identitātes pārvaldības sistēmas un privileģētas piekļuves pārvaldības programmatūra un aparatūra, arī autentifikācijas un piekļuves kontroles lasītāji, tostarp biometriskie lasītāji | Identitātes pārvaldības sistēmas ir produkti ar digitāliem elementiem, kas nodrošina autentifikācijas vai autorizācijas mehānismus un kas var nodrošināt arī mehānismus fizisku personu, juridisku personu, ierīču vai sistēmu identitātes akreditācijas datu dzīves cikla pārvaldībai, piemēram, identitātes reģistrācijai, nodrošināšanai, uzturēšanai, reģistrācijas anulēšanai. Šīs sistēmas ietver piekļuves pārvaldības sistēmas, kas kontrolē fizisku personu, juridisku personu, ierīču vai sistēmu piekļuvi digitālajiem resursiem vai fiziskajām atrašanās vietām.<br><br>Privileģētas piekļuves pārvaldības programmatūra ir piekļuves pārvaldības sistēma, kas kontrolē un uzrauga piekļuves tiesības IT vai OT sistēmām un sensitīvai informācijai organizācijā, tostarp sistēmas, kas nodrošina diferencētu piekļuves kontroles politiku privileģētiem lietotājiem.<br><br>Šajā kategorijā citstarp ietilpst autentifikācijas un piekļuves kontroles lasītāji, biometrisko datu lasītāji, vienotās pierakstīšanās programmatūra, federatīvā identitātes pārvaldības programmatūra, vienreizējas paroles programmatūra, aparatūras autentifikācijas ierīces, piemēram, darījumu autentifikācijas numura (*TAN*) ģeneratori, autentifikācijas programmatūra un daudzfaktoru autentifikācijas programmatūra. |
| 2. Atsevišķas un iegultas pārlūkprogrammas | Programmatūras produkti ar digitāliem elementiem, kas ļauj galalietotājiem piekļūt tīmekļa saturam un pakalpojumiem, kas mitināti serveros, kuri ir savienoti ar tādiem tīkliem kā internets, pārveidot tos un mijiedarboties ar tiem. Tie parasti ietver pārlūkprogrammas komponentu iezīmēšanas valodā (piemēram, *HTML*) rakstīta satura interpretēšanai un parādīšanai, atbalstu tīmekļa protokoliem (piemēram, *HTTP*, *HTTPS*), spēju izpildīt skriptus un pārvaldīt lietotāju ievadītos datus, kā arī pagaidu vai pastāvīgus datus no tīmekļa vietnēm (sīkdatnes).<br><br>Šī kategorija ietver, bet neaprobežojas ar atsevišķām lietojumprogrammām, kas pilda pārlūkprogrammu funkcijas, iegultās pārlūkprogrammas, kas paredzētas integrēšanai citā sistēmā vai lietotnē, kā arī pārlūkprogrammas ar MI aģenta integrāciju. |
| 3. Paroļu pārvaldnieki | Produkti ar digitāliem elementiem, kas uz vietas ierīcē vai attālā serverī glabā paroles, tostarp veic tādas darbības kā paroļu ģenerēšana, kā arī paroļu koplietošana un integrācija ar vietējām vai trešo personu lietotnēm paroļu izmantošanai.<br><br>Šajā kategorijā citstarp ietilpst vietējie paroļu pārvaldītāji, paroļu pārvaldnieki, kas nodrošināti kā pārlūkprogrammas paplašinājumi, uzņēmumu paroļu pārvaldnieki, kā arī aparatūras paroļu pārvaldnieki. |

| Produkta kategorija | Tehniskais apraksts |
|---|---|
| 4. Programmatūra, kas meklē, dzēš vai ievieto karantīnā ļaunprogrammatūru | Programmatūras produkti ar digitāliem elementiem, ko parasti dēvē par pretvīrusu vai ļaunatūru novēršanas programmatūru, kas atklāj vai meklē ļaunprogrammatūru vai kodu ierīcēs vai izņem vai ievieto karantīnā šādu programmatūru vai kodu, lai saglabātu šādu ierīču integritāti, konfidencialitāti vai pieejamību.<br><br>Šīs produktu kategorijas kontekstā ļaunprogrammatūra ir programmatūra ar ļaunprātīgām iezīmēm vai spējām, kas var tieši vai netieši kaitēt lietotājam un/vai datorsistēmai, piemēram, vīrusi, tārpi, izspiedējvīrusi, spiegprogrammatūra un Trojas zirgi.<br><br>Šajā kategorijā citstarp ietilpst programmatūra, kas reāllaikā vai manuāli atklāj vai meklē ļaunprogrammatūru, nosaka sistēmlaužņus un izmanto glābšanas diskus, kuru pamatfunkcija ir ļaunprogrammatūras meklēšana, dzēšana vai ievietošana karantīnā. |
| 5. Produkti ar digitāliem elementiem ar virtuālā privātā tīkla (VPN) funkciju | Produkti ar digitāliem elementiem, kas izveido šifrētu loģisku tuneli, kurš veidots no fiziska vai virtuāla tīkla sistēmas resursiem.<br><br>Šī kategorija citstarp ietver virtuālus privātus tīkla klientus, virtuālus privātus tīkla serverus un virtuālas privātas tīkla vārtejas. |
| 6. Tīkla pārvaldības sistēmas | Produkti ar digitāliem elementiem, kas pārvalda savienotus tīkla elementus, piemēram, serverus, maršrutētājus, komutatorus, darbstacijas, printerus vai mobilās ierīces, uzraugot tos un kontrolējot to tīkla darbību un konfigurāciju.<br><br>Šī kategorija citstarp ietver pārvaldības sistēmas "no gala līdz galam" un specializētas konfigurācijas pārvaldības sistēmas, piemēram, programmdefinētus tīklu kontrollerus. |
| 7. Drošības informācijas un notikumu pārvaldības (*SIEM*) sistēmas | Produkti ar digitāliem elementiem, kas vāc datus no vairākiem avotiem, analizē minētos datus un nosaka to korelācijas, kā arī nodrošina tos kā izmantojamu informāciju ar drošību saistītos nolūkos, piemēram, draudu un incidentu noteikšanas, tiesu ekspertīzes vai atbilstības nolūkos. |
| 8. Palaišanas pārvaldnieki | Programmatūras produkti ar digitāliem elementiem, kas pārvalda sistēmas sākotnējās palaišanas procesu pēc barošanas ieslēgšanas / atkārtotas iedarbināšanas ar inicializēšanas aparatūru, ielādēšanas vai vadības pārneses uz operētājsistēmas vidi vai sistēmas resursiem un sāknēšanas opciju atlases.<br><br>Šajā kategorijā citstarp ietilpst *UEFI* aparātprogrammatūra, vienpakāpes un daudzpakāpju sāknēšanas ielādētāji. |
| 9. Publiskās atslēgas infrastruktūra un digitālo sertifikātu izsniegšanas programmatūra | Produkti ar digitāliem elementiem, ko izmanto kā daļu no publiskās atslēgas infrastruktūras (*PKI*), kas pārvalda digitālo sertifikātu validēšanu, izveidi, izdošanu, izplatīšanu, statusa publicēšanu, atjaunošanu vai atsaukšanu vai ar šādiem digitālajiem sertifikātiem saistīto kriptogrāfisko atslēgu ģenerēšanu, uzglabāšanu, uzticamu glabāšanu, apmaiņu, iznīcināšanu vai rotāciju.<br><br>Šajā kategorijā citstarp ietilpst atslēgu pārvaldības sistēmas, digitālo sertifikātu pārvaldības sistēmas, tiešsaistes sertifikātu statusa protokola pieprasījumu apstrādātāji un universāli *PKI* risinājumi. |

| Produkta kategorija | Tehniskais apraksts |
|---|---|
| 10. Fiziskā un virtuālā tīkla saskarnes | Fiziskā tīkla saskarnes ir produkti ar digitāliem elementiem, kas tieši savieno ierīci ar tīklu, izmantojot lietojumprogrammu saskarni (*API*), ko nodrošina saskarnes draiveri, parasti darbojoties datraides saites līmenī, un kas ietver aparatūras adapterus uz pārsūtīšanas datu nesējiem ar atbilstošu aparātprogrammatūru, parasti darbojoties fiziskajā un datraides saites līmenī.<br><br>Virtuālās tīkla saskarnes ir produkti ar digitāliem elementiem, kas tieši vai netieši savieno ierīci ar tīklu, izmantojot *API*, kas imitē fizisko tīkla saskarņu draiveri, parasti darbojoties datraides saites līmenī.<br><br>Šajā kategorijā citstarp ietilpst vadu un bezvadu tīkla saskarnes kartes, kontrolleri un adapteri, piemēram, *Wi-Fi*, *Ethernet*, *IrDA*, *USB*, *Bluetooth*, *NearLink*, *Zigbee* vai *Fieldbus*, kā arī tīri virtuāli autonomi produkti, piemēram, virtuālā tīkla saskarnes kartes, konteineru tīkla saskarnes un *VPN* saskarnes. |
| 11. Operētājsistēmas | Programmatūras produkti ar digitāliem elementiem, kas nodrošina pamatā esošās aparatūras abstraktu saskarni un kontrolē programmatūras izpildi un kas var sniegt tādus pakalpojumus kā datošanas resursu pārvaldība un konfigurācija, plānošana, ievades-izvades kontrole, datu pārvaldība un tādas saskarnes nodrošināšana, caur kuru lietojumprogrammas mijiedarbojas ar sistēmas resursiem un perifērajām iekārtām.<br><br>Šajā kategorijā citstarp ietilpst reāllaika operētājsistēmas, vispārīga lietojuma un speciāla lietojuma operētājsistēmas. |
| 12. Maršrutētāji, modemi, kas paredzēti savienojumam ar internetu, un komutatori | Maršrutētāji ir produkti ar digitāliem elementiem, kas izveido un kontrolē datu plūsmu starp dažādiem tīkliem, izvēloties ceļus vai maršrutus, izmantojot maršrutēšanas protokola mehānismus un algoritmus, kas parasti darbojas tīkla līmenī.<br><br>Šajā kategorijā citstarp ietilpst vadu un bezvadu maršrutētāji, virtuāli maršrutētāji un maršrutētāji ar vai bez modemiem. |
| | Modemi, kas paredzēti pieslēgšanai internetam, ir aparatūras produkti ar digitāliem elementiem, kuros izmanto digitālās modulācijas un demodulācijas metodes, lai pārveidotu analogus signālus digitālajos signālos un otrādi uz IP balstītu sakaru vajadzībām.<br><br>Šajā kategorijā citstarp ietilpst optiskās šķiedras modemi, ciparu abonentlīnijas (*DSL*) modemi, kabeļu (*DOCSIS*) modemi, satelīta modemi un mobilo tīklu modemi. |
| | Komutatori ir produkti ar digitāliem elementiem, kas nodrošina savienojamību starp tīklā saslēgtām ierīcēm, izmantojot pakešu nosūtīšanas mehānismus, un kam ir pārvaldības plakne, ko parasti īsteno datraides saites vai tīkla līmenī.<br><br>Šajā kategorijā citstarp ietilpst pārvaldīti komutatori, viedie komutatori, daudzslāņu komutatori, virtuālās drošības komutatori, programmējami komutatori programmatūras definētai tīklu izveidošanai un tilti, piemēram, bezvadu piekļuves punkti. |

| Produkta kategorija | Tehniskais apraksts |
|---|---|
| 13. Mikroprocesori ar funkcijām, kas saistītas ar drošību | Produkti ar digitāliem elementiem, kas ir integrētās shēmas, kuras veic centrālās apstrādes funkcijas, izmantojot ārējo atmiņu un perifērās ierīces, ietverot mikrokodu un citu zema līmeņa aparātprogrammatūru. Turklāt tie papildus nodrošina ar drošību saistītas funkcijas, piemēram, šifrēšanu, autentifikāciju, drošu atslēgu uzglabāšanu, nejauši izvēlētu numuru ģenerēšanu, uzticamu izpildes vidi vai citus uz aparatūru balstītus aizsardzības mehānismus, kuru mērķis ir aizsargāt citus produktus, tīklus vai pakalpojumus ārpus paša mikroprocesora, piemēram, drošu sāknēšanas ķēdi, virtualizāciju vai drošas sakaru saskarnes. |
| 14. Mikrokontrolleri ar funkcijām, kas saistītas ar drošību | Produkti ar digitāliem elementiem, kas ir integrētās shēmas, kuras veic centrālas apstrādes funkcijas, integrējot atmiņu, kas ļauj mikrokontrolleram būt programmējamam, un parasti arī citas perifērās iekārtas, ietverot mikrokodu un citu zema līmeņa aparātprogrammatūru. Turklāt tie papildus nodrošina ar drošību saistītas funkcijas, piemēram, šifrēšanu, autentifikāciju, drošu atslēgu uzglabāšanu, nejauši izvēlētu numuru ģenerēšanu, uzticamu izpildes vidi vai citus uz aparatūru balstītus aizsardzības mehānismus, kuru mērķis ir aizsargāt citus produktus, tīklus vai pakalpojumus ārpus paša mikrokontrollera, piemēram, drošu sāknēšanas ķēdi, virtualizāciju vai drošas sakaru saskarnes. |
| 15. Lietojumam pielāgotas integrētās shēmas (*ASIC*) un lauka programmējamās ventiļu matricas (*FPGA*) ar funkcijām, kas saistītas ar drošību | Lietojumam pielāgotas integrētās shēmas (*ASIC*) ar funkcijām, kas saistītas ar drošību, ir produkti ar digitāliem elementiem, kas ir integrētās shēmas, kuras pilnībā vai daļēji izstrādātas pēc pasūtījuma, lai veiktu konkrētu funkciju vai īstenotu konkrētu lietojumu, ietverot mikrokodu un citu zema līmeņa aparātprogrammatūru. Turklāt tās papildus nodrošina ar drošību saistītas funkcijas, piemēram, šifrēšanu, autentifikāciju, drošu atslēgu uzglabāšanu, nejauši izvēlētu numuru ģenerēšanu, uzticamu izpildes vidi vai citus uz aparatūru balstītus aizsardzības mehānismus, kuru mērķis ir aizsargāt citus produktus, tīklus vai pakalpojumus ārpus pašas *ASIC*, piemēram, drošu sāknēšanas ķēdi, virtualizāciju vai drošas sakaru saskarnes. |
| | Lauka programmējamās ventiļu matricas (*FPGA*) ar funkcijām, kas saistītas ar drošību, ir produkti ar digitāliem elementiem, kas ir integrētās shēmas, kurām raksturīga konfigurējamu loģisko bloku matrica, kas konstruēta tā, lai pēc izgatavošanas shēmas varētu pārprogrammēt konkrētas funkcijas veikšanai vai konkrēta lietojuma īstenošanai, ietverot mikrokodu un citu zema līmeņa aparātprogrammatūru. Turklāt tās papildus nodrošina ar drošību saistītas funkcijas, piemēram, šifrēšanu, autentifikāciju, drošu atslēgu uzglabāšanu, nejauši izvēlētu numuru ģenerēšanu, uzticamu izpildes vidi vai citus uz aparatūru balstītus aizsardzības mehānismus, kuru mērķis ir aizsargāt citus produktus, tīklus vai pakalpojumus ārpus pašas *FPGA*, piemēram, drošu sāknēšanas ķēdi, virtualizāciju vai drošas sakaru saskarnes. |
| 16. Vispārēja lietojuma viedmāju virtuālie asistenti | Produkti ar digitāliem elementiem, kas tieši vai ar cita aprīkojuma starpniecību sazinās publiskajā internetā un kas apstrādā pieprasījumus, uzdevumus vai jautājumus, pamatojoties uz dabiskas valodas uzvednēm, piemēram, ar audio vai rakstveida ievadi, un kas, pamatojoties uz šiem pieprasījumiem, uzdevumiem vai jautājumiem, nodrošina piekļuvi citiem pakalpojumiem vai kontrolē savienoto ierīču funkcijas dzīvojamajās telpās.<br><br>Šī kategorija citstarp ietver viedos skaļruņus ar integrētu virtuālo asistentu un autonomus virtuālos asistentus, kas atbilst šim aprakstam. |

| Produkta kategorija | Tehniskais apraksts |
|---|---|
| 17. Viedmāju produkti ar drošības funkcijām, tostarp vieddurvju slēdzenes, videonovērošanas kameras, bērnu uzraudzības sistēmas un signalizācijas sistēmas | Produkti ar digitāliem elementiem, kas aizsargā patērētāju fizisko drošību dzīvojamā vidē un ko var kontrolēt vai pārvaldīt attālināti no citām sistēmām, kā arī aparatūra un programmatūra, kas centralizēti kontrolē šādus produktus.<br>Šajā kategorijā citstarp ietilpst vieddurvju aizslēgšanas ierīces, bērnu uzraudzības sistēmas, signalizācijas sistēmas un mājas drošības kameras. |
| 18. Internetam pieslēgtas rotaļlietas, uz kurām attiecas Eiropas Parlamenta un Padomes Direktīva 2009/48/EK ([1]) un kurām ir interaktīvas sociālas funkcijas (piemēram, runas vai filmēšanas funkcijas) vai kurām ir atrašanās vietas izsekošanas funkcijas | Internetam pieslēgtas rotaļlietas, kurām ir interaktīvas sociālas funkcijas, ir produkti ar digitāliem elementiem, uz kuriem attiecas Direktīva 2009/48/EK, kuri sazinās publiskajā internetā tieši vai ar jebkura cita aprīkojuma starpniecību un kuros ir iegultas tehnoloģijas, kas nodrošina ienākošos un izejošos sakarus, piemēram, tastatūra, mikrofons, skaļrunis vai kamera. |
| | Internetam pieslēgtas rotaļlietas, kurām ir atrašanās vietas izsekošanas funkcijas, ir produkti ar digitāliem elementiem, uz kuriem attiecas Direktīva 2009/48/EK, kuri sazinās publiskajā internetā tieši vai ar jebkura cita aprīkojuma starpniecību un kuros ir tehnoloģijas, kas ļauj izsekot vai izsecināt rotaļlietas vai tā lietotāja ģeogrāfisko atrašanās vietu. Ja rotaļlieta, izmantojot sensoru tehnoloģijas, tikai konstatē lietotāja vai citu rotaļlietu tuvumu, rotaļlieta nav uzskatāma par tādu, kurai ir atrašanās vietas izsekošanas funkcijas. |
| 19. Izstrādājumi personiskai valkāšanai, kurus paredzēts valkāt vai nēsāt uz cilvēka ķermeņa, kuri veic veselības uzraudzības (piemēram, izsekošanas) funkciju un uz kuriem neattiecas Eiropas Parlamenta un Padomes Regula (ES) 2017/745 ([2]) vai Regula (ES) 2017/746 ([3]), vai izstrādājumi personiskai valkāšanai, kuri paredzēti bērniem un kurus lieto bērni | Izstrādājumi personiskai valkāšanai, kas jāvalkā vai jānovieto uz cilvēka ķermeņa un kam ir veselības uzraudzības mērķis, ir produkti ar digitāliem elementiem, kurus valkā uz ķermeņa tieši vai ar apģērba vai aksesuāru palīdzību un kuri regulāri vai pastāvīgi var uztvert un apstrādāt lietotāja veselībai būtisku informāciju, tostarp ķermeņa rādītājus, izņemot produktus, kas ietilpst Regulas (ES) 2017/745 vai Regulas (ES) 2017/746 darbības jomā.<br>Šajā kategorijā citstarp ietilpst fiziskās aktivitātes reģistratori, viedpulksteņi, viedie juvelierizstrādājumi, viedapģērbs un sporta apģērbs, kas atbilst šim aprakstam. |
| | Izstrādājumi personiskai valkāšanai, kas paredzēti, lai tos lietotu bērni vai bērnu vajadzībām, ir produkti ar digitāliem elementiem, kurus var valkāt vai novietot uz ķermeņa tieši vai ar apģērba vai aksesuāru palīdzību personām, kas jaunākas par 14 gadiem.<br>Šī kategorija citstarp ietver valkājamus bērnu drošības līdzekļus. |

([1]) Eiropas Parlamenta un Padomes Direktīva 2009/48/EK (2009. gada 18. jūnijs) par rotaļlietu drošumu (OV L 170, 30.6.2009., 1. lpp., ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2017/745 (2017. gada 5. aprīlis), kas attiecas uz medicīniskām ierīcēm, ar ko groza Direktīvu 2001/83/EK, Regulu (EK) Nr. 178/2002 un Regulu (EK) Nr. 1223/2009 un atceļ Padomes Direktīvas 90/385/EK un 93/42/EEK (OV L 117, 5.5.2017., 1. lpp., ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Eiropas Parlamenta un Padomes Regula (ES) 2017/746 (2017. gada 5. aprīlis) par *in vitro* diagnostikas medicīniskām ierīcēm un ar ko atceļ Direktīvu 98/79/EK un Komisijas Lēmumu 2010/227/ES (OV L 117, 5.5.2017., 176. lpp., ELI: http://data.europa.eu/eli/reg/2017/746/oj).

**II klase**

| Produkta kategorija | Tehniskais apraksts |
|---|---|
| 1. Virtuālo mašīnu pārraugi un konteineru izpildlaika sistēmas, kas atbalsta operētājsistēmu un līdzīgas vides virtualizētu izpildi | Virtuālo mašīnu pārraugi ir programmatūras produkti ar digitāliem elementiem, kas izgūst un/vai sadala datošanas resursus un ļauj izpildīt, pārvaldīt un organizēt virtuālas mašīnas, kuras ir loģiski nodalītas viena no otras un/vai no fiziskās aparatūras. Virtuālo mašīnu pārraugi var darboties tieši no aparatūras (tikai iekārtās), papildus operētājsistēmām vai citā virtuālā iekārtā (ligzdota virtualizācija).<br><br>Šīs produktu kategorijas kontekstā virtuālā mašīna ir programmatūras definēta skaitļošanas vides loģiska nošķiršana, kas ietver virtuālu aparatūras resursu kopumu (piemēram, *CPU*, atmiņa, glabātuve, tīkla saskarnes) un parasti mitina savu operētājsistēmu.<br><br>Šajā kategorijā citstarp ietilpst 1. tipa virtuālie mašīnu pārraugi (tikai iekārtas), 2. tipa virtuālie mašīnu pārraugi (mitina operētājsistēmā) un hibrīdi virtuālie mašīnu pārraugi. |
| | Konteineru izpildlaika sistēmas ir programmatūras produkti ar digitāliem elementiem, kas pārvalda tādu konteineru izpildi un aprites ciklu, kuri darbojas vienā mitināšanas operētājsistēmā kā izolēti procesi, piešķir resursus un ļauj pārvaldīt un organizēt atsevišķus konteinerus.<br><br>Šīs produktu kategorijas kontekstā konteiners ir uz programmatūru balstīta izpildes vide, kas vienu vai vairākus programmatūras komponentus un to atkarības ietver vienā paketē, ļaujot tai darboties neatkarīgi un konsekventi. |
| 2. Ugunsmūri, ielaušanās atklāšanas un novēršanas sistēmas | Ugunsmūri ir produkti ar digitāliem elementiem, kas aizsargā savienotu tīklu vai sistēmu no neatļautas piekļuves, uzraugot un ierobežojot datu sakaru plūsmu uz minēto tīklu un no tā.<br><br>Šajā kategorijā citstarp ietilpst tīkla ugunsmūri un lietojumprogrammu ugunsmūri, piemēram, tīmekļa lietojumprogrammu ugunsmūri vai filtri un surogātpasta vārtejas. |
| | Ielaušanās atklāšanas sistēmas ir produkti ar digitāliem elementiem, kas uzrauga datplūsmu pēc tam, kad tā ir nonākusi tīkla vidē, lai noteiktu aizdomīgas darbības, un atklāj vai konstatē, ka ir noticis ielaušanās mēģinājums vai arī ielaušanās notiek vai ir notikusi savienotā tīklā vai sistēmā.<br><br>Šajā kategorijā citstarp ietilpst uz tīklu balstītas ielaušanās atklāšanas sistēmas un uz mitinātāju balstītas ielaušanās atklāšanas sistēmas. |
| | Ielaušanās novēršanas sistēmas ir produkti ar digitāliem elementiem, kas sastāv no ielaušanās atklāšanas sistēmas, kura aktīvi reaģē uz ielaušanos savienotā tīklā vai sistēmā.<br><br>Šajā kategorijā citstarp ietilpst uz tīklu balstītas ielaušanās novēršanas sistēmas un uz mitinātāju balstītas ielaušanās novēršanas sistēmas. |

| Produkta kategorija | Tehniskais apraksts |
|---|---|
| 3. Pret iejaukšanos droši mikroprocesori | Produkti ar digitāliem elementiem, kas ir mikroprocesori ar šā pielikuma tabulas "I klase" 13. punktā minētajām ar drošību saistītām funkcijām, tostarp pierādījumiem par neatļautām darbībām, noturību vai reakciju, un kas papildus ir paredzēti, lai nodrošinātu AVA_VAN 2. vai 3. līmeņa aizsardzību, kā noteikts vienotajos kritērijos un vienotajā izvērtēšanas metodikā. |
| 4. Pret iejaukšanos droši mikrokontrolleri | Produkti ar digitāliem elementiem, kas ir mikrokontrolleri ar šā pielikuma tabulas "I klase" 14. punktā minētajām ar drošību saistītām funkcijām, tostarp pierādījumiem par neatļautām darbībām, noturību vai reakciju, un kas papildus ir paredzēti, lai nodrošinātu AVA_VAN 2. vai 3. līmeņa aizsardzību, kā noteikts vienotajos kritērijos un vienotajā izvērtēšanas metodikā. |





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

*II PIELIKUMS*

**KRITISKI SVARĪGI PRODUKTI AR DIGITĀLIEM ELEMENTIEM**

| Produkta kategorija | Tehniskais apraksts |
|---|---|
| 1. Aparatūras ierīces ar drošības blokiem | Aparatūras produkti ar digitāliem elementiem, kas droši glabā, apstrādā vai pārvalda sensitīvus datus vai veic kriptogrāfiskas darbības un kas sastāv no vairākiem diskrētiem komponentiem, kuri ietver aparatūras fizisko apvalku, kas nodrošina pierādījumus par iejaukšanos, kā arī noturību vai reakciju kā pretpasākumus pret fiziskiem uzbrukumiem.<br><br>Šī kategorija citstarp ietver fiziskus maksājumu terminālus, aparatūras drošības moduļus, kas ģenerē un pārvalda kriptogrāfijas elementus, un tahogrāfus, kas atbilst iepriekš minētajam aprakstam. |
| 2. Viedo skaitītāju vārtejas, kas ir daļa no viedās uzskaites sistēmām, kas definētas Eiropas Parlamenta un Padomes Direktīvas (ES) 2019/944 ([1]) 2. panta 23. punktā, un citas ierīces augstas drošības nolūkiem, tostarp drošai kriptoapstrādei | Viedo skaitītāju vārtejas ir produkti ar digitāliem elementiem, kuri kontrolē saziņu starp komponentiem viedās uzskaites sistēmās vai kas ir savienoti ar viedās uzskaites sistēmām, kas definētas Direktīvas (ES) 2019/944 2. panta 23. punktā, un pilnvarotām trešām personām, piemēram, komunālo pakalpojumu sniedzējiem. Viedo skaitītāju vārtejas vāc, apstrādā un glabā skaitītāju vai personas datus, aizsargā datus un informācijas plūsmas, atbalstot konkrētas kriptogrāfijas vajadzības, piemēram, datu šifrēšanu un atšifrēšanu, ietver ugunsmūra funkcijas un nodrošina līdzekļus citu ierīču vadībai.<br><br>Šī kategorija citstarp ietver viedo skaitītāju vārtejas, kas saistītas ar viedās uzskaites sistēmām, kuras mēra elektroenerģiju, kā definēts Direktīvas (ES) 2019/944 2. panta 23. punktā. Tā var ietvert arī viedo skaitītāju vārtejas, ko izmanto citās viedajās uzskaites sistēmās, ar ko mēra citu enerģijas avotu, piemēram, gāzes vai siltuma, patēriņu, ar nosacījumu, ka vārteja atbilst šim aprakstam. |
| 3. Viedkartes vai līdzīgas ierīces, ieskaitot to drošības elementus | Drošības elementi ir mikrokontrolleri vai mikroprocesori ar funkcijām, kas saistītas ar drošību un kas ietver pierādījumus par iejaukšanos, kā arī noturību vai reakciju. Parasti tie glabā, apstrādā vai pārvalda kriptogrāfiskās darbības vai sensitīvus datus, piemēram, identitātes akreditācijas datus vai maksājumu akreditācijas datus. Drošības elementi ir paredzēti, lai nodrošinātu vismaz AVA_VAN.4 aizsardzību, kā noteikts vienotajos kritērijos vai vienotajā novērtēšanas metodikā. Tie var būt silīcija pusvadītāju komponenti vai tikt integrēti mikroshēmu (*SoC*) ķēdēs. Drošības elementi var ietvert lietojumprogrammu vidi vai operētājsistēmu, kā arī vienu vai vairākas lietojumprogrammas.<br><br>Šajā kategorijā citstarp ietilpst uzticamo platformu moduļi (*TPM*) un iegultā universālā integrālās shēmas karte (*UICC*). |
| | Viedkartes vai līdzīgas ierīces ir drošības elementi, kas integrēti nesējmateriālā, piemēram, plastmasā vai kokā, kas ir kartes formā, vai drošības elementi, kas integrēti citas formas nesējmateriālos.<br><br>Šajā kategorijā citstarp ietilpst identitātes un ceļošanas dokumenti, kvalificētas paraksta kartes, aizstājamas *UICC*, fiziskas maksājumu kartes, fiziskas piekļuves kartes, digitālo tahogrāfu kartes vai aproces ar integrētiem maksājumu drošības elementiem. |

([1]) Eiropas Parlamenta un Padomes Direktīva (ES) 2019/944 (2019. gada 5. jūnijs) par kopīgiem noteikumiem attiecībā uz elektroenerģijas iekšējo tirgu un ar ko groza Direktīvu 2012/27/ES (OV L 158, 14.6.2019., 125. lpp., ELI: http://data.europa.eu/eli/dir/2019/944/oj).