REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/2392 AL COMISIEI

din 28 noiembrie 2025

privind descrierea tehnică a categoriilor de produse importante și critice cu elemente digitale în temeiul Regulamentului (UE) 2024/2847 al Parlamentului European și al Consiliului

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) ([1]), în special articolul 7 alineatul (4),

întrucât:

(1) Regulamentul (UE) 2024/2847 stabilește norme privind securitatea cibernetică a produselor cu elemente digitale. În particular, anexa III la regulamentul respectiv stabilește categoriile de produse importante cu elemente digitale care, atunci când sunt introduse pe piață, fac obiectul unor proceduri de evaluare a conformității mai stricte decât cele aplicabile altor produse cu elemente digitale. Anexa IV la Regulamentul (UE) 2024/2847 stabilește categoriile de produse critice cu elemente digitale pentru care producătorii ar putea fi obligați să obțină un certificat european de securitate cibernetică în cadrul unui sistem european de certificare a securității cibernetice în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului ([2]) sau care ar face obiectul unei evaluări obligatorii a conformității de către o parte terță la introducerea pe piață.

(2) În temeiul articolului 7 alineatul (1) și al articolului 8 alineatul (1) din Regulamentul (UE) 2024/2847, funcționalitatea de bază a unui produs cu elemente digitale stabilește dacă produsul cu elemente digitale respectiv corespunde descrierii tehnice a unei categorii de produse importante sau critice cu elemente digitale și, în consecință, dacă acesta face obiectul procedurilor aplicabile de evaluare a conformității.

(3) Atunci când dezvoltă un produs cu elemente digitale, producătorii integrează de regulă în propriile lor produse cu elemente digitale, pentru a obține setul dorit de funcționalități, alte componente care sunt la rândul lor produse cu elemente digitale și care pot corespunde descrierii tehnice a unei categorii de produse importante sau critice. În conformitate cu Regulamentul (UE) 2024/2847, un produs cu elemente digitale face obiectul procedurilor de evaluare a conformității aplicabile produselor importante sau critice cu elemente digitale dacă produsul respectiv în ansamblul său este un produs important sau critic, astfel cum se prevede în anexele III și IV la regulamentul respectiv. De exemplu, includerea unui browser încorporat ca o componentă a unei aplicații de știri destinate utilizării în telefoane inteligente nu face, în sine, ca aplicația de știri să facă obiectul procedurii de evaluare a conformității aplicabile produselor cu elemente digitale care au funcționalitatea de bază „browsere autonome și încorporate”. Cu toate acestea, în conformitate cu Regulamentul (UE) 2024/2847, producătorul trebuie să se asigure că produsul cu elemente digitale în ansamblu îndeplinește cerințele esențiale de securitate cibernetică. Prin urmare, producătorul trebuie să evalueze securitatea întregului produs, ținând cont, după caz, de securitatea componentelor sau a funcționalităților care sunt integrate în acesta. De exemplu, pentru ca producătorul unei aplicații de știri să demonstreze că produsul său cu elemente digitale este conform cu Regulamentul (UE) 2024/2847, producătorul respectiv trebuie să demonstreze că aplicația de știri în ansamblul său îndeplinește cerințele aplicabile, ținând cont, după caz, de securitatea browserului încorporat care este integrat în aplicația sa.

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

([2]) Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Faptul că un produs cu elemente digitale îndeplinește funcții diferite sau suplimentare față de cele detaliate în descrierile tehnice prevăzute în prezentul regulament nu înseamnă, în sine, că produsul cu elemente digitale nu are funcționalitatea de bază a unei categorii de produse prevăzute în anexele III și IV la Regulamentul (UE) 2024/2847. De exemplu, produsele cu elemente digitale care au funcționalitatea de bază „sisteme de operare” includ adesea componente software care îndeplinesc funcții auxiliare ce nu sunt incluse în descrierea tehnică a respectivei categorii de produse, cum ar fi aplicațiile pentru făcut calcule sau programele de editare grafică simple. Produsele cu elemente digitale încorporează adesea și componente care au funcționalitatea unui alt produs important sau critic cu elemente digitale, cum ar fi un sistem de operare care integrează o funcție de browser sau un router care integrează o funcție de firewall. Totuși, acest lucru nu înseamnă, în sine, că astfel de produse cu elemente digitale nu au funcționalitatea de bază „sisteme de operare” sau, respectiv, „routere, modemuri destinate conectării la internet și comutatoare”.

(5) Pe de altă parte, se consideră că un produs cu elemente digitale care are capacitatea de a îndeplini funcțiile unei categorii de produse prevăzute în anexele III și IV la Regulamentul (UE) 2024/2847, dar a cărui funcționalitate de bază este diferită de cea a unei astfel de categorii de produse, nu corespunde descrierii tehnice a respectivei categorii de produse. De exemplu, un software de orchestrare, automatizare și răspuns în materie de securitate (*security orchestration, automation and response* – SOAR) are adesea capacitatea de a îndeplini funcțiile produselor cu elemente digitale din categoria „sisteme de gestionare a informațiilor de securitate și a evenimentelor de securitate (SIEM)”, și anume de a colecta date, de a le analiza și de a le prezenta ca informații care pot fi luate pentru a lua măsuri în scopuri de securitate. Cu toate acestea, întrucât funcționalitatea sa de bază nu este cea a unui SIEM, nu trebuie, în general, să se considere că software-ul SOAR corespunde descrierii tehnice a „sistemelor de gestionare a informațiilor de securitate și a evenimentelor de securitate (SIEM)”. În mod similar, un telefon inteligent integrează, de regulă, componente care îndeplinesc funcțiile mai multor categorii de produse prevăzute în anexele III și IV la Regulamentul (UE) 2024/2847, cum ar fi un sistem de operare sau un manager de parole integrat. Cu toate acestea, întrucât funcționalitatea de bază a unui telefon inteligent nu este cea de sistem de operare sau de manager de parole, se consideră, în general, că telefonul inteligent nu corespunde descrierii tehnice a unor astfel de categorii de produse.

(6) În conformitate cu articolul 13 alineatele (2) și (3) din Regulamentul (UE) 2024/2847, producătorii de produse cu elemente digitale trebuie să pună în aplicare cerințele esențiale de securitate cibernetică prevăzute în partea I din anexa I la Regulamentul (UE) 2024/2847 într-un mod proporțional cu riscurile produsului cu elemente digitale în cauză, pe baza scopului preconizat și a utilizării previzibile în mod rezonabil, precum și a condițiilor de utilizare a produsului cu elemente digitale, ținând seama de durata preconizată a utilizării produsului. În conformitate cu articolul 13 alineatele (2) și (3) din regulamentul respectiv și indiferent dacă produsul cu elemente digitale este considerat a fi un produs important sau critic cu elemente digitale, producătorii trebuie să efectueze o evaluare cuprinzătoare a riscurilor în materie de securitate cibernetică și să indice modul în care cerințele esențiale de securitate cibernetică sunt puse în aplicare pe baza evaluării riscurilor, inclusiv în ceea ce privește testarea și asigurarea acestora. În cazul în care funcționalitatea de bază a produsului lor cu elemente digitale corespunde descrierii tehnice a unui produs important sau critic cu elemente digitale, producătorii trebuie să demonstreze conformitatea urmând procedurile specifice de evaluare a conformității stabilite la articolul 32 alineatele (2), (3), (4) și (5) din Regulamentul (UE) 2024/2847.

(7) Prezentul regulament include exemple de produse cu elemente digitale a căror funcționalitate de bază corespunde descrierii tehnice a anumitor produse importante sau critice cu elemente digitale. Astfel de exemple sunt furnizate doar în scopuri ilustrative și nu reprezintă o listă exhaustivă.

(8) Pentru a oferi securitate juridică producătorilor, categoriile de produse cu elemente digitale, inclusiv elemente de securitate, „microprocesoare rezistente la manipulare frauduloasă”, „microcontrolere rezistente la manipulare frauduloasă”, „carduri inteligente și dispozitive similare” ar trebui să fie diferențiate în funcție de nivelul de rezistență la o potențială exploatare a defectelor sau a deficiențelor pentru care au fost proiectate. Nivelul AVA_VAN este o modalitate utilizată pe scară largă și standardizată de a exprima un astfel de nivel de rezistență. Nivelurile AVA_VAN sunt stabilite în standardele privind criteriile comune și metodologia comună de evaluare disponibile publicului, care stau la baza cadrelor de certificare adoptate pe scară largă pe piață, cum ar fi Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei ([3]). Regulamentul de punere în aplicare (UE) 2024/482 stabilește un sistem european de

([3]) Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei din 31 ianuarie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

certificare a securității cibernetice care poate fi utilizat pentru certificarea unui produs ca îndeplinind un anumit nivel de asigurare. Inspirându-se din practicile observate la nivel global, Regulamentul de punere în aplicare (UE) 2024/482 prevede posibilitatea emiterii, până la sfârșitul anului 2027, de certificate bazate pe versiuni mai vechi ale standardelor. Prin urmare, în contextul Regulamentului (UE) 2024/2847, este oportun să se permită ca nivelurile AVA_VAN să fie exprimate prin trimitere fie la cea mai recentă versiune, fie la versiuni mai vechi ale standardelor respective.

(9) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit în temeiul articolului 62 alineatul (1) din Regulamentul (UE) 2024/2847,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „criterii comune” înseamnă criteriile comune pentru evaluarea securității tehnologiei informației, astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul de punere în aplicare (UE) 2024/482 sau astfel cum sunt prevăzute în standardele menționate la articolul 3 alineatul (2) literele (a) și (b) din regulamentul de punere în aplicare respectiv;
2. „metodologie comună de evaluare” înseamnă metodologia comună de evaluare a securității informatice, astfel cum este definită la articolul 2 punctul 2 din Regulamentul de punere în aplicare (UE) 2024/482 sau astfel cum se prevede în standardele menționate la articolul 3 alineatul (2) literele (c) și (d) din regulamentul de punere în aplicare respectiv.

Articolul 2

(1) Descrierea tehnică a categoriilor de produse cu elemente digitale din clasele I și II enumerate în anexa III la Regulamentul (UE) 2024/2847 este prevăzută în anexa I la prezentul regulament.

(2) Descrierea tehnică a categoriilor de produse cu elemente digitale enumerate în anexa IV la Regulamentul (UE) 2024/2847 este prevăzută în anexa II la prezentul regulament.

Articolul 3

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 28 noiembrie 2025.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

PRODUSELE IMPORTANTE CU ELEMENTE DIGITALE

Clasa I

Categoria de produse	Descrierea tehnică
1. Software și hardware pentru sisteme de gestionare a identității și de gestionare a accesului privilegiat, inclusiv cititoare de autentificare și de control al accesului, inclusiv cititoare biometrice	Sistemele de gestionare a identității sunt produse cu elemente digitale care oferă mecanisme de autentificare sau autorizare și care pot oferi, de asemenea, mecanisme de gestionare a ciclului de viață al credențialelor de autentificare ale persoanelor fizice, ale persoanelor juridice, ale dispozitivelor sau ale sistemelor, cum ar fi înregistrarea, furnizarea, întreținerea și radierea identității. Aceste sisteme includ sisteme de gestionare a accesului care controlează accesul persoanelor fizice, al persoanelor juridice, al dispozitivelor sau al sistemelor la resurse digitale sau la locații fizice. Software-urile de gestionare a accesului privilegiat sunt sisteme de gestionare a accesului care controlează și monitorizează drepturile de acces la sistemele IT sau OT și la informațiile sensibile din cadrul unei organizații, inclusiv sistemele care pun în aplicare politici diferențiate de control al accesului pentru utilizatorii privilegiați. Această categorie include, fără a se limita la acestea, cititoarele de autentificare și de control al accesului, cititoarele biometrice, software-ul de autentificare unică (*Single Sign-On*), software-ul federat de gestionare a identității, software-ul de generat parole unice, dispozitivele hardware de autentificare, cum ar fi generatoarele de numere de autentificare a tranzacției (*transaction autentificare number* – TAN), software-ul de autentificare și software-ul de autentificare multifactorială.
2. Browsere autonome și încorporate	Produse software cu elemente digitale care permit utilizatorilor finali să acceseze, să redea și să interacționeze cu conținutul și serviciile web găzduite pe servere conectate la rețele precum internetul. Acestea includ, de regulă, un motor de browser pentru interpretarea și afișarea conținutului scris într-un limbaj de marcare (de exemplu HTML), suport pentru protocoale web (de exemplu HTTP sau HTTPS), capacitatea de a executa scripturi și de a gestiona textul introdus de utilizatori, precum și stocarea de date temporare sau persistente de pe site-uri (cookie-uri). Această categorie include, dar nu se limitează la aplicațiile de sine stătătoare care îndeplinesc funcțiile browserelor, browserele încorporate destinate integrării într-un alt sistem sau într-o altă aplicație, precum și browserele în care sunt integrați agenți IA.
3. Manageri de parole	Produse cu elemente digitale care stochează parole, la nivel local pe un dispozitiv sau pe un server la distanță, incluzând funcții precum generarea de parole și partajarea parolelor și integrarea cu aplicații locale sau terțe pentru utilizarea parolelor. Această categorie include, dar nu se limitează la managerii de parole locali, managerii de parole puși la dispoziție ca extensii ale browserelor, managerii de parole de întreprindere, precum și managerii de parole bazați pe hardware.

Categoria de produse	Descrierea tehnică
4. Software care caută, elimină sau plasează în carantină programe informatice malware	Produse software cu elemente digitale, denumite de obicei antivirus sau antimalware, care detectează sau caută programe sau cod malware pe dispozitive sau elimină sau plasează în carantină un astfel de program, pentru a menține integritatea, confidențialitatea sau disponibilitatea unor astfel de dispozitive. În contextul acestei categorii de produse, program malware înseamnă un program care conține caracteristici sau capacități rău-intenționate care pot cauza prejudicii direct sau indirect utilizatorului și/sau sistemului informatic, cum ar fi virusuri, viermi informatici, ransomware, programe spion și troiani. Această categorie include, dar nu se limitează la software care detectează sau caută programe malware în timp real sau manual, diskuri de detectare și salvare de tip rootkit cu funcționalitatea de bază de căutare, eliminare sau plasare în carantină a programelor malware.
5. Produse cu elemente digitale cu funcție de rețea privată virtuală (VPN)	Produse cu elemente digitale care stabilesc un tunel logic criptat construit din resursele de sistem ale unei rețele fizice sau virtuale. Această categorie include, dar nu se limitează la clienții de rețea virtuală privată (VPN), serverele de rețea virtuală privată și gateway-urile de rețea virtuală privată.
6. Sisteme de administrare a rețelei	Produse cu elemente digitale care gestionează elemente de rețea conectate, cum ar fi servere, routere, comutatoare, stații de lucru, imprimante sau dispozitive mobile, prin monitorizarea acestora și controlarea funcționării și configurării lor în rețea. Această categorie include, dar nu se limitează la sistemele de gestionare de la un capăt la altul și sistemele dedicate de gestionare a configurației, cum ar fi controlerele pentru crearea de rețele definite prin software.
7. Sisteme de gestionare a informațiilor de securitate și a evenimentelor de securitate (SIEM)	Produse cu elemente digitale care colectează date din surse multiple, analizează și corelează datele respective și le prezintă ca informații care pot fi puse în aplicare în scopuri legate de securitate, cum ar fi detectarea amenințărilor și a incidentelor, analiza criminalistică sau asigurarea conformității.
8. Manageri de boot	Produse software cu elemente digitale care gestionează procesul de pornire inițială a sistemului după pornirea/repornirea sistemului, prin inițializarea hardware-ului, încărcarea sau transferul controlului către mediul sistemului de operare sau resursele sistemului și selectarea opțiunilor de boot. Această categorie include, dar nu se limitează la firmware UEFI și bootloader-e cu un singur stadiu sau cu mai multe stadii.
9. Infrastructuri publice esențiale și software pentru emiterea de certificate digitale	Produsele cu elemente digitale utilizate ca parte a unei infrastructuri de chei publice (PKI) care gestionează validarea, crearea, emiterea, distribuirea, publicarea statutului, reînnoirea sau revocarea certificatelor digitale sau generarea, stocarea, plasarea în escrow, schimbul, distrugerea sau rotația cheilor criptografice asociate cu astfel de certificate digitale. Această categorie include, dar nu se limitează la sistemele de gestionare a cheilor, sistemele de gestionare a certificatelor digitale, sistemele de răspuns la cererile din cadrul protocoalelor de verificare online a statutului certificatelor și soluțiile PKI de tip *all-in-one*.

Categoria de produse	Descrierea tehnică
10. Interfețe fizice și virtuale de rețea	Interfețele fizice de rețea sunt produse cu elemente digitale care conectează direct un dispozitiv la o rețea prin intermediul unei interfețe de programare a aplicațiilor (API) furnizate de driverele interfeței, care funcționează de regulă la nivelul legăturii de date și care au adaptoare hardware la suporturile de transmisie echipate cu firmware corespunzător, funcționând de obicei la nivelul fizic și la nivelul legăturii de date. Interfețele virtuale de rețea sunt produse cu elemente digitale care conectează direct sau indirect un dispozitiv la o rețea prin intermediul unei API care o imită pe cea a driverelor interfețelor fizice de rețea, funcționând de obicei la nivelul legăturii de date. Această categorie include, dar nu se limitează la carduri de interfață de rețea cu fir și fără fir, controlere și adaptoare, cum ar fi pentru Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee sau Fieldbus, precum și produse autonome pur virtuale, cum ar fi cardurile de interfață virtuală de rețea, interfețele de rețea în containere și interfețele VPN.
11. Sisteme de operare	Produse software cu elemente digitale care oferă o interfață abstractă cu hardware-ul subiacent și controlează executarea software-ului și care pot furniza servicii precum gestionarea și configurarea resurselor informatice, programarea, controlul intrărilor și al ieșirilor, gestionarea datelor și furnizarea unei interfețe prin care aplicațiile interacționează cu resursele sistemului și cu perifericele. Această categorie include, dar nu se limitează la sistemele de operare în timp real, sistemele de operare de uz general și sistemele de operare cu destinație specială.
12. Routere, modemuri destinate conectării la internet și comutatoare	Routerele sunt produse cu elemente digitale care stabilesc și controlează fluxul de date dintre diferite rețele prin selectarea căilor sau a rutelor utilizând mecanisme și algoritmi de protocol de rutare, funcționând de obicei la nivelul rețelei. Această categorie include, dar nu se limitează la routerele cu fir și fără fir, routerele virtuale și routerele cu sau fără modemuri.
	Modemurile destinate conectării la internet sunt produse hardware cu elemente digitale care utilizează tehnici de modulare și demodulare digitală pentru a converti semnalele analogice în, respectiv din semnale digitale pentru comunicarea bazată pe protocolul IP. Această categorie include, dar nu se limitează la modemuri pentru fibră optică, modemuri pentru linie de abonat digitală (DSL), modemuri pentru cablu (DOCSIS), modemuri pentru satelit și modemuri celulare.
	Comutatoarele sunt produse cu elemente digitale care asigură conectivitatea între dispozitivele din rețea prin mecanisme de transmitere a pachetelor și care au o componentă de gestionare, de regulă implementată la nivelul legăturii de date sau al rețelei. Această categorie include, dar nu se limitează la comutatoare gestionate, comutatoare inteligente, comutatoare multistrat, comutatoare de securitate virtuale, comutatoare programabile pentru rețele definite prin software și punți, cum ar fi punctele de acces fără fir.

Categoria de produse	Descrierea tehnică
13. Microprocesoare cu funcționalități legate de securitate	Produse cu elemente digitale care sunt circuite integrate ce îndeplinesc funcții centrale de procesare bazate pe memorie externă și periferice, inclusiv microcod și alte tipuri de firmware de nivel scăzut. În plus, acestea oferă funcționalități legate de securitate, cum ar fi criptarea, autentificarea, stocarea securizată a cheilor, generarea aleatorie de numere, un mediu de executare de încredere sau alte mecanisme de protecție bazate pe hardware care vizează securizarea altor produse, rețele sau servicii dincolo de microprocesorul în sine, cum ar fi o secvență de bootare securizată, virtualizarea sau interfețele de comunicare securizate.
14. Microcontrolere cu funcționalități legate de securitate	Produse cu elemente digitale care sunt circuite integrate ce îndeplinesc funcții centrale de procesare și care au o memorie integrată ce permite programarea microcontrolerului și, în mod tipic, și a altor periferice, inclusiv microcod și alte tipuri de firmware de nivel scăzut. În plus, acestea oferă funcționalități legate de securitate, cum ar fi criptarea, autentificarea, stocarea securizată a cheilor, generarea aleatorie de numere, un mediu de executare de încredere sau alte mecanisme de protecție bazate pe hardware care vizează securizarea altor produse, rețele sau servicii dincolo de microcontrolerul în sine, cum ar fi o secvență de bootare securizată, virtualizarea sau interfețele de comunicare securizate.
15. Circuite integrate specifice aplicațiilor (ASIC) și rețele de porți programabile de utilizator (FPGA) cu funcționalități legate de securitate	Circuitele integrate specifice aplicațiilor (ASIC) cu funcționalități legate de securitate sunt produse cu elemente digitale care sunt circuite integrate concepute integral sau parțial pentru a îndeplini o funcție specifică sau pentru a implementa o aplicație specifică, inclusiv microcod și alte tipuri de firmware de nivel scăzut. În plus, acestea oferă funcționalități legate de securitate, cum ar fi criptarea, autentificarea, stocarea securizată a cheilor, generarea aleatorie de numere, un mediu de executare de încredere sau alte mecanisme de protecție bazate pe hardware care vizează securizarea altor produse, rețele sau servicii dincolo de ASIC în sine, cum ar fi o secvență de bootare securizată, virtualizarea sau interfețele de comunicare securizate.
	Circuitele integrate programabile de către utilizator (FPGA) cu funcționalități legate de securitate sunt produse cu elemente digitale care sunt circuite integrate caracterizate de o matrice de blocuri logice configurabile concepute pentru a fi reprogramabile după producere pentru a îndeplini o funcție specifică sau pentru a implementa o aplicație specifică, inclusiv microcod și alte tipuri de firmware de nivel scăzut. În plus, acestea oferă funcționalități legate de securitate, cum ar fi criptarea, autentificarea, stocarea securizată a cheilor, generarea aleatorie de numere, un mediu de executare de încredere sau alte mecanisme de protecție bazate pe hardware care vizează securizarea altor produse, rețele sau servicii dincolo de FPGA în sine, cum ar fi o secvență de bootare securizată, virtualizarea sau interfețele de comunicare securizate.
16. Asistenți virtuali de uz general pentru locuințe inteligente	Produsele cu elemente digitale care comunică pe internetul public, fie direct, fie prin intermediul altor echipamente, care procesează cereri, sarcini sau întrebări formulate într-un limbaj natural, cum ar fi pe cale audio sau în scris, și care, pe baza acestor cereri, sarcini sau întrebări, oferă acces la alte servicii sau controlează funcțiile unor dispozitive conectate în contexte rezidențiale. Această categorie include, dar nu se limitează la difuzoarele inteligente cu un asistent virtual integrat și asistenții virtuali de sine stătători care corespund acestei descrieri.

Categoria de produse	Descrierea tehnică
17. Produse pentru locuințe inteligente cu funcționalități legate de securitate, inclusiv încuietori inteligente ale ușilor, camere de securitate, sisteme de monitorizare a bebelușilor și sisteme de alarmă	Produse cu elemente digitale care protejează securitatea fizică a consumatorilor într-un mediu rezidențial și care pot fi controlate sau gestionate de la distanță de alte sisteme, precum și hardware-ul și software-ul care controlează la nivel central astfel de produse. Această categorie include, dar nu se limitează la dispozitivele inteligente de încuiere a ușilor, sistemele de monitorizare a bebelușilor, sistemele de alarmă și camerele de securitate pentru locuințe.
18. Jucării conectate la internet care intră sub incidența Directivei 2009/48/CE a Parlamentului European și a Consiliului ([1]), care au caracteristici sociale interactive (de exemplu, vorbire sau filmare) sau care au funcții de localizare	Jucăriile conectate la internet care au caracteristici sociale interactive sunt produse cu elemente digitale care intră sub incidența Directivei 2009/48/CE și care comunică pe internetul public, fie direct, fie prin intermediul oricărui alt echipament, și care au tehnologii integrate ce permit comunicarea către și dinspre dispozitiv, cum ar fi tastatură, microfon, difuzor sau cameră video.
	Jucăriile conectate la internet care au funcții de localizare sunt produse cu elemente digitale care intră sub incidența Directivei 2009/48/CE și care comunică pe internetul public, fie direct, fie prin intermediul oricărui alt echipament, și care au tehnologii care permit urmărirea sau deducerea locației geografice a jucăriei sau a utilizatorului acesteia. În cazul în care jucăria nu face decât să detecteze proximitatea utilizatorului sau a altor jucării prin utilizarea tehnologiilor de detecție, se consideră că jucăria nu are caracteristici de localizare și urmărire.
19. Produse purtabile personale care urmează să fie purtate sau plasate pe un corp uman care au un scop de monitorizare a stării de sănătate (cum ar fi urmărirea) și cărora nu li se aplică Regulamentul (UE) 2017/745 ([2]) sau (UE) 2017/746 ([3]) al Parlamentului European și al Consiliului, sau produse purtabile personale care sunt destinate utilizării de către și pentru copii	Produsele purtabile personale destinate să fie purtate sau plasate pe un corp uman care au un scop de monitorizare a stării de sănătate sunt produse cu elemente digitale care sunt purtate pe corp direct sau prin îmbrăcăminte sau accesorii și care pot, în mod regulat sau continuu, să capteze și să proceseze informații relevante pentru sănătatea utilizatorului, inclusiv parametri corporali, cu excepția produselor care intră în domeniul de aplicare al Regulamentului (UE) 2017/745 sau al Regulamentului (UE) 2017/746. Această categorie include, dar nu se limitează la dispozitivele de urmărire a activității fizice, ceasurile inteligente, bijuteriile inteligente, îmbrăcămintea inteligentă și îmbrăcămintea sportivă care corespund acestei descrieri.
	Produsele purtabile personale destinate utilizării de către și pentru copii sunt produse cu elemente digitale care pot fi purtate sau plasate pe corpul persoanelor cu vârsta sub 14 ani, direct sau prin îmbrăcăminte sau accesorii. Această categorie include, dar nu se limitează la dispozitivele purtabile de siguranță pentru copii.

([1]) Directiva 2009/48/CE a Parlamentului European și a Consiliului din 18 iunie 2009 privind siguranța jucăriilor (JO L 170, 30.6.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic *in vitro* și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Clasa II

Categoria de produse	Descrierea tehnică
1. Hipervizoare și sisteme de runtime a containerelor care sprijină executarea virtualizată a sistemelor de operare și a mediilor similare	Hipervizoarele sunt produse software cu elemente digitale care abstrag și/sau alocă resurse informatice și care permit executarea, gestionarea și orchestrarea mașinilor virtuale care sunt separate logic unele de altele și/sau de hardware-ul fizic. Hipervizoarele pot rula direct pe hardware (*bare metal*), printr-un sistem de operare sau în cadrul unei alte mașini virtuale (virtualizare imbricată). În contextul acestei categorii de produse, o mașină virtuală este un compartiment logic definit prin software al unui mediu informatic, care include un set virtualizat de resurse hardware (de exemplu CPU, memorie, stocare și interfețe de rețea) și are, de regulă, propriul sistem de operare. Această categorie include, dar nu se limitează la hipervizoarele de tip 1 (*bare metal*), hipervizoarele de tip 2 (găzduite într-un sistem de operare) și hipervizoarele hibride.
	Sistemele de executare (*runtime*) a containerelor sunt produse software cu elemente digitale care gestionează executarea și ciclul de viață al containerelor care rulează pe un singur sistem de operare gazdă ca procese izolate, alocând resursele și permițând gestionarea și orchestrarea containerelor individuale. În contextul acestei categorii de produse, un container este un mediu de executare bazat pe software care încapsulează una sau mai multe componente software și dependențele acestora într-un singur pachet, permițându-i să funcționeze independent și consecvent.
2. Firewall-uri, sisteme de detectare și prevenire a intruziunilor	Firewall-urile sunt produse cu elemente digitale care protejează o rețea conectată sau un sistem conectat împotriva accesului neautorizat prin monitorizarea și restricționarea traficului de comunicații de date către și dinspre rețeaua respectivă. Această categorie include, dar nu se limitează la firewall-urile de rețea și firewall-urile pentru aplicații, cum ar fi firewall-urile pentru aplicații web sau filtrele și gateway-urile antispam.
	Sistemele de detectare a intruziunilor sunt produse cu elemente digitale care monitorizează traficul odată ce acesta a intrat în mediul rețelei, pentru a identifica activități suspecte, și detectează sau identifică faptul că s-a încercat, este în curs de producere sau s-a produs o intruziune într-o rețea conectată sau un sistem conectat. Această categorie include, dar nu se limitează la sistemele de detectare a intruziunilor bazate pe rețea și bazate pe gazdă.
	Sistemele de prevenire a intruziunilor sunt produse cu elemente digitale compuse dintr-un sistem de detectare a intruziunilor care răspunde în mod activ la o intruziune într-o rețea conectată sau un sistem conectat. Această categorie include, dar nu se limitează la sistemele de prevenire a intruziunilor de la nivelul rețelei și sistemele de prevenire a intruziunilor de la nivelul gazdei.

Categoria de produse	Descrierea tehnică
3. Microprocesoare rezistente la manipulare frauduloasă	Produse cu elemente digitale care sunt microprocesoare cu funcționalități legate de securitate menționate în tabelul „Clasa I” punctul 13 din prezenta anexă, inclusiv indicii ale manipulării frauduloase, rezistență la manipulare frauduloasă sau reacție la manipulare frauduloasă, și care, în plus, sunt concepute pentru a asigura o protecție AVA_VAN de nivelul 2 sau 3, astfel cum se prevede în criteriile comune și în metodologia comună de evaluare.
4. Microcontrolere rezistente la manipulare frauduloasă	Produse cu elemente digitale care sunt microcontrolere cu funcționalități legate de securitate menționate în tabelul „Clasa I” punctul 14 din prezenta anexă, inclusiv indicii ale manipulării frauduloase, rezistență la manipulare frauduloasă sau reacție la manipulare frauduloasă, și care, în plus, sunt concepute pentru a asigura o protecție AVA_VAN de nivelul 2 sau 3, astfel cum se prevede în criteriile comune și în metodologia comună de evaluare.

ANEXA II

PRODUSELE CRITICE CU ELEMENTE DIGITALE

Categoria de produse	Descrierea tehnică
1. Dispozitive hardware cu casete de securitate	Produse hardware cu elemente digitale care stochează, procesează sau gestionează în condiții de siguranță date sensibile sau efectuează operațiuni criptografice și care constau în mai multe componente distincte, încorporând un înveliș fizic hardware care oferă indicii ale manipulării frauduloase, rezistență la manipulare frauduloasă sau reacție la manipulare frauduloasă drept contramăsuri împotriva atacurilor fizice. Această categorie include, dar nu se limitează la terminalele fizice de plată, modulele de securitate hardware care generează și gestionează elemente criptografice și tahografele care corespund descrierii de mai sus.
2. Gateway-urile contoarelor inteligente din cadrul sistemelor de contorizare inteligentă în sensul definiției de la articolul 2 punctul 23 din Directiva (UE) 2019/944 a Parlamentului European și a Consiliului [1] și alte dispozitive utilizate în scopuri avansate de securitate, inclusiv pentru procesarea criptografică securizată	Gateway-urile contoarelor inteligente sunt produse cu elemente digitale care controlează comunicarea dintre componente ale sistemelor de contorizare inteligentă sau conectate la acestea, astfel cum sunt definite la articolul 2 punctul 23 din Directiva (UE) 2019/944, și părțile terțe autorizate, cum ar fi furnizorii de utilități. Gateway-urile contoarelor inteligente colectează, procesează și stochează date provenite de la contoare sau date cu caracter personal, protejează fluxurile de date și informații răspunzând unor nevoi criptografice specifice, cum ar fi criptarea și decriptarea datelor, încorporează funcționalități de firewall și oferă mijloacele de control al altor dispozitive. Această categorie include, dar nu se limitează la gateway-urile contoarelor inteligente aferente sistemelor de contorizare inteligentă care măsoară energia electrică, astfel cum sunt definite la articolul 2 punctul 23 din Directiva (UE) 2019/944. Categoria poate include, de asemenea, gateway-urile pentru contoare inteligente utilizate în alte sisteme de contorizare inteligentă care măsoară consumul altor surse de energie, cum ar fi gazele sau căldura, cu condiția ca gateway-ul respectiv să corespundă acestei descrieri.
3. Carduri inteligente sau dispozitive similare, inclusiv elemente de securitate	Elementele de securitate sunt microcontrolere sau microprocesoare cu funcționalități legate de securitate, inclusiv indicii ale manipulării frauduloase, rezistență la manipulare frauduloasă sau reacție la manipulare frauduloasă. De regulă acestea stochează, procesează sau gestionează operațiuni criptografice sau date sensibile, cum ar fi credențialele de autentificare sau de plată. Elementele de securitate sunt concepute pentru a oferi protecție la un nivel cel puțin egal cu AVA_VAN.4, astfel cum se prevede în criteriile comune sau în metodologia comună de evaluare. Acestea pot fi cipuri distincte sau pot fi integrate în sisteme pe cip (*System on a Chip* – SoC). Elementele de securitate pot încorpora un mediu de aplicație sau un sistem de operare și pot include una sau mai multe aplicații. Această categorie include, dar nu se limitează la modulele de platformă de încredere (*Trusted Platform Modules* – TPM) și cardurile inteligente universale (*Universal Integrated Circuit Card* – UICC) încorporate.
	Cardurile inteligente sau dispozitivele similare sunt elemente de securitate integrate într-un material suport, cum ar fi plasticul sau lemnul, sub forma unui card, sau elemente de securitate integrate în materiale suport având alte forme. Această categorie include, dar nu se limitează la documentele de identitate și de călătorie, cardurile de semnătură calificate, UICC care pot fi înlocuite, cardurile fizice de plată, cardurile fizice de acces, cardurile de tahograf digital sau brățările cu elemente de securitate a plăților integrate.

[1] Directiva (UE) 2019/944 a Parlamentului European și a Consiliului din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).