Europeiska unionens
officiella tidning

SV
L-serien

2025/2392

1.12.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/2392

av den 28 november 2025

om den tekniska beskrivningen av kategorierna av viktiga och kritiska produkter med digitala element enligt Europaparlamentets och rådets förordning (EU) 2024/2847

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) ([1]), särskilt artikel 2.5 andra stycket, och

av följande skäl:

(1) I förordning (EU) 2024/2847 fastställs cybersäkerhetsregler för produkter med digitala element. I bilaga III till den förordningen anges kategorier av viktiga produkter med digitala element som, när de släpps ut på marknaden, omfattas av förfaranden för bedömning av överensstämmelse som är striktare än de förfaranden som tillämpas på andra produkter med digitala element. I bilaga IV till förordning (EU) 2024/2847 anges kategorier av kritiska produkter med digitala element för vilka tillverkare kan åläggas att erhålla ett europeiskt cybersäkerhetscertifikat inom ramen för en europeiska ordning för cybersäkerhetscertifiering enligt Europaparlamentets och rådets förordning (EU) 2019/881 ([2]) eller som kan omfattas av en tredjepartsbedömning av överensstämmelse, när de släpps ut på marknaden.

(2) Enligt artikel 7.1 och artikel 8.1 i förordning (EU) 2024/2847 är det kärnfunktionen hos en produkt med digitala element som avgör om produkten med digitala element motsvarar den tekniska beskrivningen för en kategori av viktiga eller kritiska produkter med digitala element och därmed omfattas av de tillämpliga förfarandena för bedömning av överensstämmelse.

(3) När tillverkarna utvecklar en produkt med digitala element integrerar de, för att uppnå den önskade uppsättningen funktioner, vanligtvis andra komponenter i sina egna produkter med digitala element, och även dessa kan motsvara den tekniska beskrivningen för en kategori av viktiga eller kritiska produkter. Enligt förordning (EU) nr 2024/2847 omfattas en produkt med digitala element av de förfaranden för bedömning av överensstämmelse som är tillämpliga på viktiga eller kritiska produkter med digitala element, om produkten som helhet är en viktig eller kritisk produkt enligt bilagorna III och IV till den förordningen. Exempelvis innebär inte integrering av en inbäddad webbläsare som komponent i en nyhetsapp för användning i smarttelefoner i sig att nyhetsappen omfattas av det förfarande för bedömning av överensstämmelse som är tillämpligt på produkter med digitala element som har kärnfunktionen hos ”Fristående och inbyggda webbläsare”. I enlighet med förordning (EU) 2024/2847 måste dock tillverkaren säkerställa att produkten med digitala element som helhet uppfyller de väsentliga cybersäkerhetskraven. Tillverkaren behöver utvärdera säkerheten för hela produkten och, såsom lämpligt, beakta säkerheten för de komponenter eller funktioner som är integrerade i den. För att en tillverkare av en nyhetsapp ska anses visa att dennes produkt med digitala element är i överensstämmelse med förordning (EU) nr 2024/2847 måste tillverkaren till exempel visa att nyhetsappen som helhet uppfyller de tillämpliga kraven, med beaktande, såsom lämpligt, av säkerheten för den inbäddade webbläsare som är integrerad i nyhetsappen.

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

([2]) Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Det faktum att en produkt med digitala element utför andra funktioner än de som anges i de tekniska beskrivningarna eller funktioner utöver dessa innebär inte i sig att produkten med digitala element inte har kärnfunktionen hos en produktkategori som anges i bilagorna III och IV i förordning (EU) 2024/2847. Produkter med digitala element som har kärnfunktionen hos ”operativsystem” omfattar ofta programvara som utför kompletterande funktioner som inte ingår i den tekniska beskrivningen för den produktkategorin, såsom räknare eller enkla grafikredigerare. Produkter med digitala element innehåller också komponenter med samma funktioner som en annan viktig eller kritisk produkt med digitala element, t.ex. ett operativsystem som integrerar webbläsarfunktioner eller en router som integrerar brandväggsfunktioner. Detta innebär dock inte i sig att sådana produkter med digitala element inte har kärnfunktionen hos ”operativsystem” respektive ”routrar, modem avsedda för anslutning till internet och dataväxlar”.

(5) Samtidigt kan inte en produkt med digitala element med förmåga att utföra funktionerna hos en produktkategori som anges i bilagorna III och IV i förordning (EU) 2024/2847, men vars själva kärnfunktion är en annan än för denna produktkategori, anses motsvara den tekniska beskrivningen av den produktkategorin. Exempelvis har programvara för orkestrering, automatisering och åtgärdande (SOAR) ofta kapacitet att utföra funktionerna hos produkter med digitala element i kategorin ”system för säkerhetsinformation och händelsehantering (SIEM)”, dvs. att samla in, analysera och presentera data som handlingsbar information för säkerhetsändamål. SOAR-programvarans kärnfunktion är dock inte densamma som för SIEM, eftersom SOAR-programvaran i allmänhet inte anses motsvara den tekniska beskrivningen för ”system för säkerhetsinformation och händelsehantering (SIEM)”. Likaså innehåller en smarttelefon vanligtvis komponenter som utför funktionerna hos flera produktkategorier som anges i bilagorna III och IV till förordning (EU) 2024/2847, t.ex. operativsystem eller integrerade lösenordshanterare. I och med att en smarttelefons kärnfunktion inte är densamma som ett operativsystems eller en lösenordhanterares anses den dock i allmänhet inte motsvara den tekniska beskrivningen för dessa produktkategorier.

(6) I enlighet med artikel 13.2 och 13.3 i förordning (EU) 2024/2847 ska tillverkarna av produkter med digitala element genomföra de väsentliga cybersäkerhetskrav som anges i del I i bilaga I till förordning (EU) 2024/2847 på ett sätt som står i proportion till riskerna hos produkten med digitala element, baserat på det avsedda syftet med produkten med digitala element samt dess rimligen förutsebara användning och användarvillkor, med beaktande av hur länge produkten förväntas vara i bruk. I enlighet med artikel 13.2 och 13.3 i den förordningen, och oavsett om produkten med digitala element anses vara en viktig eller kritisk produkt med digitala element, ska tillverkarna göra en omfattande bedömning av cybersäkerhetsriskerna och ange hur de väsentliga cybersäkerhetskraven ska genomföras med beaktande av riskbedömningen, inbegripet testning och assurans. I de fall där kärnfunktionen hos produkten med digitala element motsvarar den tekniska beskrivningen för en viktig eller kritisk produkt med digitala element ska tillverkaren visa produktens överensstämmelse i enlighet med de särskilda förfaranden för bedömning av överensstämmelse som fastställs i artikel 32.2, 32.3, 32.4 och 32.5 i förordning (EU) 2024/2847.

(7) I denna förordning anges exempel på produkter med digitala element vars kärnfunktion motsvarar den tekniska beskrivningen för vissa viktiga eller kritiska produkter med digitala element. De anges endast som illustrativa exempel och utgör inte någon uttömmande förteckning.

(8) Med tanke på tillverkarnas rättssäkerhet bör kategorier av produkter med digitala element som är manipuleringssäkra mikroprocessorer, manipuleringssäkra mikrokontroller samt smartkort och liknande produkter, inbegripet säkra element, särskiljas baserat på den nivå av motståndskraft mot potentiella möjligheter att utnyttja fel eller svagheter som de utformats för. AVA_VAN-nivå är ett allmänt använt och standardiserat sätt att uttrycka en sådan nivå av motståndskraft. AVA_VAN-nivåer fastställs i de allmänt tillgängliga standarderna för Common Criteria och gemensam evalueringsmetodik, som ligger till grund för befintliga certifieringsramar som anammats brett på marknaden, såsom kommissionens genomförandeförordning (EU) 2024/482 ([3]). Genom genomförandeförordning

([3]) Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(EU) 2024/482 inrättas en europeisk ordning för cybersäkerhetscertifiering som kan användas för certifiering av en produkt baserat på dess assuransnivå. Baserat på global praxis omfattar genomförandeförordning (EU) 2024/482 möjligheten att utfärda certifikat baserade på äldre versioner av standarderna till utgången av 2027. Inom ramen för förordning (EU) 2024/2847 är det därför lämpligt att tillåta att AVA_VAN-nivåer uttrycks med hänvisning till antingen den senaste versionen eller äldre versioner av dessa standarder.

(9) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats i enlighet med artikel 62.1 i förordning (EU) 2024/2847.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Definitioner

I denna förordning gäller följande definitioner:

(1) *Common Criteria*: de gemensamma kriterierna för utvärdering av informationsteknologisk säkerhet enligt definitionen i artikel 2.1 i genomförandeförordning (EU) 2024/482 eller enligt de standarder som avses i artikel 3.2 a och b i den genomförandeförordningen.

(2) *gemensam evalueringsmetodik*: den gemensamma metoden för utvärdering av informationsteknologisk säkerhet enligt definitionen i artikel 2.2 i genomförandeförordning (EU) 2024/482 eller enligt de standarder som avses i artikel 3.2 c och d i den genomförandeförordningen.

Artikel 2

1. Den tekniska beskrivningen av kategorier av produkter med digitala element i klasserna I och II som anges i bilaga III till förordning (EU) nr 2024/2847 ska vara den som anges i bilaga I till den här förordningen.

2. Den tekniska beskrivningen av kategorier av produkter med digitala element i bilaga IV till förordning (EU) nr 2024/2847 ska vara den som anges i bilaga II till den här förordningen.

Artikel 3

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 28 november 2025.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA I

VIKTIGA PRODUKTER MED DIGITALA ELEMENT

Klass I

Produktkategori	Teknisk beskrivning
1. Identitetshanteringssystem och programvara och hårdvara för hantering av privilegierad åtkomst, inbegripet läsare för autentisering och åtkomstkontroll, inbegripet biometriska läsare	Identitetshanteringssystem är produkter med digitala element som tillhandahåller mekanismer för autentisering och auktorisationskontroller och som också kan tillhandahålla mekanismer för livscykelhantering av identitetsuppgifter för fysiska personer, juridiska personer, enheter eller system, såsom registrering, tillhandahållande, underhåll och avregistrering av identitetsuppgifter. Dessa system omfattar åtkomsthanteringssystem som kontrollerar fysiska personers, juridiska personers, enheters eller systems åtkomst till digitala resurser eller fysiska platser. Programvara för hantering av privilegierad åtkomst är ett åtkomsthanteringssystem som kontrollerar och övervakar åtkomsträttigheter till it- eller OT-system och känsliga uppgifter i en organisation, inbegripet system för verkställande av differentierade policyer för åtkomstkontroll när det gäller privilegierade användare. Denna kategori inbegriper, men är inte begränsad till, läsare för autentisering och åtkomstkontroll, biometriska läsare, programvara för samlad inloggning (SSO), programvara för federerad identitetshantering, programvara för engångslösenord, hårdvara för autentisering av enheter såsom generatorer av transaktionsautentiseringsnummer (TAN), autentiseringsprogramvara och programvara för flerfaktorsautentisering.
2. Fristående och inbyggda webbläsare	Programvaruprodukter med digitala element som gör det möjligt att få åtkomst till, återge, och interagera med webbinnehåll och tjänster som finns på servrar som är anslutna till nätverk som t.ex. internet. Dessa omfattar vanligen en webbläsarmotor för att tolka och visa innehåll skrivet på märkspråk (t.ex. HTML), stöd för webbprotokoll (t.ex. HTTP, HTTPS), förmåga att köra skript och hantera användarindata samt lagring av tillfälliga eller beständiga data från webbplatser (kakor). Denna kategori omfattar, men är inte begränsad till, fristående applikationer som fyller funktion som webbläsare, inbäddade webbläsare avsedda för integrering i andra system eller applikationer samt webbläsare med integrerad AI-agent.
3. Lösenordshanterare	Produkter med digitala element som lagrar lösenord, lokalt på en enhet eller på en fjärrserver, inklusive sådant som generering av lösenord, delning av lösenord och integrering av lösenord med lokala applikationer eller tredjepartsapplikationer för lösenordsanvändning. Denna kategori omfattar, men är inte begränsad till, lokala lösenordshanterare, lösenordshanterare som tillhandahålls som webbläsartillägg samt hårdvarubaserade lösenordshanterare.

Produktkategori	Teknisk beskrivning
4. Programvara som söker efter och avlägsnar skadlig programvara eller sätter den i karantän	Programvaruprodukter med digitala element, normalt benämnda antivirus- eller antimalware-program, som upptäcker eller söker efter sabotageprogram eller -koder eller -enheter, eller som avlägsnar sådana programvaror eller koder eller sätter dem i karantän, för att upprätthålla integriteten, konfidentialiteten eller tillgängligheten för sådana enheter. När det gäller denna produktkategori, betyder sabotageprogram programvara som innehåller fientliga funktioner eller förmågor som direkt eller indirekt kan orsaka användaren och/eller datorsystemet skada, t.ex. virus, maskar, utpressningsprogram, spionprogram och trojaner. Denna kategori omfattar, men är inte begränsad till, programvara som upptäcker eller söker efter sabotageprogram i realtid eller manuellt, spökprogram och räddningsdiskar (rescue disks) med kärnfunktionen att söka eller avlägsna sabotageprogram eller sätta dem i karantän.
5. Produkter med digitala element vilka fungerar som virtuella privata nätverk (VPN)	Produkter med digitala element som upprättar en krypterad logisk tunnel konstruerad av systemresurserna hos ett fysiskt eller virtuellt nätverk. Denna kategori omfattar, men är inte begränsad till, virtuella privata klientnätverk, virtuella privata nätservrar och virtuella privata nätportar.
6. System för nätverkshantering	Produkter med digitala element som hanterar nätelement, såsom servrar, routrar, omkopplare, arbetsstationer, skrivare eller mobila enheter, genom att övervaka dem och kontrollera deras nätverksdrift och konfiguration. Denna kategori omfattar, men är inte begränsad till, hanteringssystem från ändpunkt till ändpunkt och konfigurationshanteringssystem, såsom styrenheter för programvarudefinierad nätverksdrift.
7. System för säkerhetsinformation och händelsehantering (SIEM)	Produkter med digitala element som samlar in data från flera källor, analyserar och korrelerar dessa data och presenterar dem som handlingsbar information för säkerhetsrelaterade ändamål, såsom detektering av hot och incidenter, forensisk analys och efterlevnad.
8. Starthanterare	Programvaruprodukter med digitala element som hanterar systemprocessen vid start/omstart genom att de initialiserar hårdvaran, laddar operativssystemmiljön eller systemresurser respektive överför kontrollen till dessa och väljer startalternativ. Denna kategori omfattar, men är inte begränsad till, UEFI-firmware, enstegs- eller flerstegsstarthanterare.
9. Infrastruktur för kryptering med öppen nyckel (PKI) och programvara för utfärdande av digitala certifikat	Produkter med digitala element vilka används som en del i en PKI-infrastruktur som hanterar validering, skapande, utfärdande statuspublicering, förnyande eller återkallande av digitala certifikat eller generering, lagring, deponering, utbyte, förstöring eller rotation av krypteringsnycklar förbundna med sådana digitala certifikat. Denna kategori omfattar, men är inte begränsad till, nyckelhanteringssystem, system för hantering av digitala certifikat, svarsenheter för onlineprotokoll avseende onlinestatus (online certificate status protocol responders) och allt i ett-PKI-lösningar.

Produktkategori	Teknisk beskrivning
10. Fysiska och virtuella nätverksgränssnitt	Fysiska nätverksgränssnitt är produkter med digitala element som direkt kopplar en enhet till ett programmeringsgränssnitt (API) som tillhandahålls av gränssnittsdrivrutiner, vilka normalt används i datalänkskiktet, och som har hårdvaruadaptrar till överföringsmedier med motsvarande firmware, som vanligtvis används i det fysiska skiktet och datalänkskiktet. Virtuella nätverksgränssnitt är produkter med digitala element som direkt eller indirekt kopplar en enhet till ett nätverk via ett programmeringsgränssnitt som efterliknar drivrutinerna hos fysiska nätverksgränssnitt, som normalt används i datalänkskiktet. Denna kategori omfattar men är inte begränsade till nätverkskort för trådnät och trådlösa nät, styrenheter och adaptrar, t.ex. för wifi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee eller Fieldbus samt rent virtuella fristående produkter, t.ex. nätverkskort för virtuella nätverk, container-nätverksgränssnitt och VPN-gränssnitt.
11. Operativsystem	Programvaruprodukter med digitala element som tillhandahåller ett abstrakt gränssnitt för den underliggande hårdvaran och kontrollerar körning av programvara och som kan tillhandahålla sådana tjänster som hantering av datorresurser och konfigurering, schemaläggning, input-output-kontroll, datahantering och tillhandahållande av ett gränssnitt, genom vilket applikationer kan interagera med systemresurser och kringutrustning. Denna kategori omfattar, men är inte begränsad till, realtidsoperativsystem och operativsystem för allmänna och särskilda ändamål.
12. Routrar, modem avsedda för anslutning till internet och dataväxlar	Routrar och produkter med digitala element som upprättar och kontrollerar dataflödet mellan olika nätverk genom att välja olika vägar eller rutter med användning av dirigeringsprotokollmekanismer och algoritmer, som normalt drivs i nätverksskiktet. Denna kategori omfattar, men är inte begränsade till, trådbundna eller trådlösa routrar, virtuella routrar och routrar med eller utan modem.
	Modem avsedda för anslutning till internet är hårdvaruprodukter med digitala element som använder digital modulerings- och demoduleringsteknik för att omvandla analoga signaler till digitala signaler, eller vice versa, för IP-baserad kommunikation. Denna kategori omfattar, men är inte begränsade till, fibermodem, DSL-modem (Digital Subscriber Line), kabelmodem (DOCSIS), satellitmodem och mobilmodem.
	Omkopplare är produkter med digitala element som tillhandahåller konnektivitet mellan nätverksanslutna enheter genom paketförmedlingsmekanismer och som har ett hanteringsplan (management plane), vanligtvis i datalänkssskiktet eller nätverksskiktet. Denna kategori omfattar, men är inte begränsad till, hanterade omkopplare, smarta omkopplare, multiskiktsomkopplare (multilayer switches), virtuella säkerhetsomkopplare, programmerbara omkopplare för programvarudefinierade nätverk och bryggor såsom trådlösa accesspunkter.

Produktkategori	Teknisk beskrivning
13. Mikroprocessorer med säkerhetsrelaterade funktioner	Produkter med digitala element som är integrerade kretsar som utför centrala behandlingsfunktioner som förlitar sig på externt minne och kringutrustning, inklusive mikrokod och annan lågnivå-firmware. De tillhandahåller också säkerhetsrelaterade funktioner såsom kryptering, autentisering, säker lagring av nycklar, slumptalsgenerering, tillförlitlig miljö för körning eller andra hårdvarubaserade skyddsmekanismer, som syftar till att säkra andra produkter, nätverk eller tjänster utöver själva mikroprocessorn, såsom säker botkedja eller virtualisering eller säkra kommunikationsgränssnitt.
14. Mikrokontroller med säkerhetsrelaterade funktioner	Produkter med digitala element vilka är integrerade kretsar som utför centrala behandlingsfunktioner vilka integrerar minne, så att mikrokontrollerna är programmerbara och normalt även annan kringutrustning inklusive mikrokod och annan lågnivå-firmware. De tillhandahåller också säkerhetsrelaterade funktioner såsom kryptering, autentisering, säker lagring av nycklar, slumptalsgenerering, tillförlitlig miljö för körning eller andra hårdvarubaserade skyddsmekanismer, som syftar till att säkra andra produkter, nätverk eller tjänster utöver själva mikrokontrollern, såsom säker botkedja eller virtualisering eller säkra kommunikationsgränssnitt.
15. Applikationsspecifika integrerade kretsar (ASIC) och fältprogrammerbara grindmatriser (FPGA) med säkerhetsrelaterade funktioner	Applikationsspecifika integrerade kretsar (ASIC) med säkerhetsrelaterade funktioner är produkter med digitala element som är integrerade kretsar, helt eller delvis skräddarsydda för att utföra en specifik funktion eller genomföra den specifik tillämpning, inbegripet mikrokod och annan lågnivå-firmware. De tillhandahåller också säkerhetsrelaterade funktioner såsom kryptering, autentisering, säker lagring av nycklar, slumptalsgenerering, tillförlitlig miljö för körning eller andra hårdvarubaserade skyddsmekanismer, som syftar till att säkra andra produkter, nätverk eller tjänster utöver ASIC i sig, såsom säker botkedja eller virtualisering eller säkra kommunikationsgränssnitt.
	FPGA (Field-programmable gate arrays) med säkerhetsrelaterade funktioner är produkter med digitala element som är integrerade kretsar som kännetecknas av en matris eller konfigurerbara logikblock (CLB) utformade för att vara omprogrammerbara efter tillverkningen för att utföra en specifik funktion eller genomföra den specifik tillämpning, inbegripet mikrokod och annan lågnivå-firmware. De tillhandahåller också säkerhetsrelaterade funktioner såsom kryptering, autentisering, säker lagring av nycklar, slumptalsgenerering, tillförlitlig miljö för körning eller andra hårdvarubaserade skyddsmekanismer, som syftar till att säkra andra produkter, nätverk eller tjänster utöver FPGA i sig, såsom säker botkedja eller virtualisering eller säkra kommunikationsgränssnitt.
16. Smarta virtuella assistenter för allmänna ändamål	Produkter med digitala element som kommunicerar via offentligt internet, direkt eller via annan utrustning, som behandlar uppmaningar, uppdrag eller frågor baserat på promptar på naturliga språk, såsom indata i form av ljud eller skrift, och som baserat på dessa uppmaningar, uppdrag eller frågor ger tillgång till andra tjänster eller kontrollerar funktioner för uppkopplade enheter i hemmiljö. Denna kategori omfattar, men är inte begränsad till, smarta högtalare med en integrerad virtuell assistent eller fristående virtuella assistenter som motsvarar denna beskrivning.

Produktkategori	Teknisk beskrivning
17. Smarta hemprodukter med säkerhetsfunktioner, inbegripet smarta dörrlås, säkerhetskameror, babyövervakningssystem och larmsystem	Produkter med digitala element som skyddar konsumenters fysiska säkerhet i hemmiljö och som kan kontrolleras eller hanteras på distans från andra system samt hårdvara och programvara som kontrollerar sådana produkter centralt. Denna kategori omfattar, men är inte begränsad till, smarta dörrlåsningsanordningar, babyövervakningssystem, larmsystem och hemsäkerhetskameror.
18. Internetanslutna leksaker som omfattas av Europaparlamentets och rådets direktiv 2009/48/EG ([1]) och som har sociala interaktiva funktioner (t.ex. tal eller filmning) eller som har positionsspårningsfunktioner	Internetanslutna leksaker med socialt interaktiva funktioner är produkter med digitala element som omfattas av direktiv 2009/48/EG, vilka kommunicerar på det offentliga internet, antingen direkt eller via annan utrustning, och som har inbäddad teknik som möjliggör inkommande och utgående kommunikation, såsom tangentbord, mikrofon, högtalare eller kamera
	Internetanslutna leksaker med positionsspårningsfunktioner är produkter med digitala element som omfattas av direktiv 2009/48/EG, vilka kommunicerar på det offentliga internet, antingen direkt eller via annan utrustning, och har teknik som möjliggör spårning eller härledning av leksakens eller dess ägares position. Om leksaken detekterar närheten till användaren eller andra leksaker endast med hjälp av avkänningsteknik anses leksaken inte ha någon positionsspårningsfunktion.
19. Personliga kroppsburna produkter som ska bäras eller placeras på en människokropp och som har ett hälsoövervakningssyfte (t.ex. spårning) och som inte omfattas av förordning (EU) 2017/745 ([2]) eller Europaparlamentets och rådets förordning (EU) 2017/746 ([3]), eller personliga kroppsburna produkter som är avsedda att användas av och för barn	Personliga kroppsburna produkter som ska bäras eller placeras på en människokropp och som har ett hälsoövervakningssyfte är produkter med digitala element som bärs på direkt på kroppen eller via klädesplagg eller accessoarer och som regelbundet eller kontinuerligt kan känna igen och behandla information, inklusive biometriska kroppsdata, som är relevanta för användarens hälsa, exklusive produkter som omfattas av förordning (EU) 2017/745 eller förordning (EU) 2017/746. Denna kategori omfattar, men är inte begränsad till, aktivitetsmätare, smartklockor, smarta smycken, smarta klädesplagg och smarta sportartiklar som motsvarar denna beskrivning.
	Personliga kroppsburna produkter som är avsedda för användning av och för barn är produkter med digitala element som kan bäras eller placeras på kroppen, direkt eller via klädesplagg eller accessoarer, för individer som är under 14 år. Denna kategori omfattar, men är inte begränsad till, kroppsburna barnsäkerhetsprodukter.

([1]) Europaparlamentets och rådets direktiv 2009/48/EG av den 18 juni 2009 om leksakers säkerhet (EUT L 170, 30.6.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för *in vitro*-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Klass II

Produktkategori	Teknisk beskrivning
1. Hypervisorer och system för körning av programcontainrar som stöder virtualiserad exekvering av operativsystem och liknande miljöer	Hypervisorer är programvaruprodukter med digitala element som abstraherar och/eller tilldelar datorresurser och som möjliggör exekvering, hantering och orkestrering av virtuella maskiner som är logiskt separerade från varandra och/eller från fysisk hårdvara. Hypervisorer kan köras direkt på hårdvara (bare metal), över ett operativsystem eller inom en annan virtuell maskin (kapslad virtualisering). Inom denna produktkategori är en virtuell maskin en programvarudefinierad logisk avgränsning av en datormiljö, som omfattar en virtualiserad uppsättning hårdvaruresurser (t.ex. CPU, minne, lagring nätverksgränssnitt) och som normalt har sitt eget operativsystem. Denna kategori omfattar, men är inte begränsad till, hypervisorer av typ 1 (bare metal), hypervisorer av typ 2 (används på ett operativsystem) och hybridhypervisorer.
	System för körning av programbehållare är programvaruprodukter med digitala element som hanterar exekvering och livscykel för behållare som körs på ett enda värdoperativsystem som isolerade processer och som fördelar resurser och tillåter hantering och orkestrering av enskilda containrar. Inom denna produktkategori är en container en programvarubaserad exekveringsmiljö som kapslar in en eller flera programvarukomponenter och av dem avhängiga element (dependencies) i ett enda paket, som gör att den kan köras fristående och konsekvent.
2. Brandväggar, intrångsdetektions- och intrångsskyddssystem	Brandväggar är produkter med digitala element som skyddar ett uppkopplat nätverk eller system från obehörig åtkomst genom övervakning och begränsning av datakommunikationstrafiken till och från det nätverket. Denna kategori omfattar, men är inte begränsad till, nätverksbrandväggar och applikationsbrandväggar såsom webbapplikationsbrandväggar eller -filter och nätslussar mot skräppost.
	Intrångsdetektionssystem är produkter med digitala element som övervakar trafik när den har kommit in i nätverksmiljön för att upptäcka misstänkt aktivitet och som detekterar och identifierar intrångsförsök och intrång som inträffar eller har inträffat i ett uppkopplat nätverk eller system. Denna kategori omfattar, men är inte begränsad till, nätverksbaserade intrångsdetektionssystem och värdbaserade intrångsdetektionssystem.
	Intrångsdetektionssystem är produkter med digitala element som består av ett intrångsdetektionssystem vilka aktivt reagerar på ett intrång i ett uppkopplat nätverk eller system. Denna kategori omfattar, men är inte begränsad till, nätverksbaserade system för intrångsskydd och värdbaserade system för intrångsskydd.

Produktkategori	Teknisk beskrivning
3. Manipulationssäkra mikroprocessorer	Produkter med digitala element som är mikroprocessorer med säkerhetsrelaterade funktioner som avses i tabellen ”Klass I”, punkt 13 i denna bilaga, inbegripet bevis på manipulering, motstånd mot manipulering eller svarsåtgärd mot manipulering, och som dessutom är utformade för att skydda AVA_VAN-nivå 2 eller 3, i enlighet med Common Criteria och den gemensamma evalueringsmetodiken.
4. Manipulationssäkra mikrokontroller	Produkter med digitala element som är mikrokontroller med säkerhetsrelaterade funktioner som avses i tabellen ”Klass I”, punkt 14 i denna bilaga, inbegripet bevis på manipulering, motstånd mot manipulering eller svarsåtgärd mot manipulering, och som dessutom är utformade för att skydda AVA_VAN-nivå 2 eller 3, i enlighet med Common Criteria och den gemensamma evalueringsmetodiken.

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

BILAGA II

KRITISKA PRODUKTER MED DIGITALA ELEMENT

Produktkategori	Teknisk beskrivning
1. Hårdvaruenheter med säkerhetsboxar	Hårdvaruprodukter med digitala element som på ett säkert sätt lagrar, behandlar eller hanterar känsliga data eller utför kryptografiska operationer, eller som består av flera diskreta komponenter, inkorporerar ett fysiskt hårdvaruhölje som tillhandahåller bevis på manipulering, motstånd mot manipulering eller svarsåtgärd mot manipulering som motåtgärder mot fysiska attacker. Denna kategori omfattar, men är inte begränsad till, fysiska betalningsterminaler, säkerhetsmoduler i hårdvara som genererar och hantera kryptografiska element samt färdskrivare som motsvarar beskrivningen ovan.
2. Smarta mätarportar inom smarta mätarsystem enligt definitionen i artikel 2.23 i Europaparlamentets och rådets direktiv (EU) 2019/944 ([1]) och andra enheter för avancerade säkerhetsändamål, inbegripet för säker kryptobehandling	Smarta mätarportar är produkter med digitala element som kontrollerar kommunikation mellan komponenter i eller anslutna till smarta mätarsystem enligt definitionen i artikel 2.23 i direktiv (EU) 2019/944 och auktoriserade tredje parter, såsom leverantörer av allmännyttiga tjänster. Smarta mätarportar samlar in, behandlar och lagra mätardata eller personuppgifter, skyddar data och informationsflöden genom att stödja specifika kryptografiska behov, såsom kryptering av data, innefattar brandväggsfunktioner och ger möjlighet att kontrollera andra anordningar. Denna kategori omfattar, men är inte begränsad till, smarta mätarportar för smarta mätarsystem för elektricitet enligt definitionen i artikel 2.23 i direktiv (EU) 2019/944. Den kan också omfatta smarta mätarportar som används i andra smarta mätarsystem som mäter förbrukningen av andra energikällor såsom gas eller värme, förutsatt att porten motsvarar denna beskrivning.
3. Smartkort eller liknande enheter, inbegripet säkra element	Säkra element är mikrokontroller eller mikroprocessorer med säkerhetsrelaterade funktioner, inbegripet på manipulering, motstånd mot manipulering eller svarsåtgärder mot manipulering. De lagrar, behandlar eller hanterar vanligtvis kryptografiska operationer eller känsliga data, såsom identitetsuppgifter eller betalningsuppgifter. Säkra element är utformade för att ge skydd på minst AVA_VAN.4-nivå, i enlighet med Common Criteria och den gemensamma evalueringsmetodiken. De kan utgöras av diskret kisel eller kan vara integrerade i system på chip. Säkra element kan inbegripa en applikationsmiljö eller ett operativsystem och kan omfatta en eller flera applikationer. Denna kategori omfattar, men är inte begränsad till, Trusted Platform Modules (TPM) och inbäddade universalkort med integrerade kretsar (Universal Integrated Circuit Card, UICC).
	Smartkort eller liknande anordningar är säkra element integrerade i ett bärarmaterial, såsom plast eller trä, i form av ett kort, eller säkra element integrerade i bärarmaterial som tar andra former. Denna kategori omfattar men är inte begränsade till id- och resehandlingar, kvalificerade kort för underskrifter, ersättningsbara UICC, fysiska betalkort, fysiska tillträdeskort, digitala färdskrivarkort eller armband med integrerade säkra betalningselement.

([1]) Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).