Publicatieblad
van de Europese Unie

NL
L-serie

2025/2392

1.12.2025

UITVOERINGSVERORDENING (EU) 2025/2392 VAN DE COMMISSIE

van 28 november 2025

betreffende de technische beschrijving van de categorieën belangrijke en kritieke producten met digitale elementen krachtens Verordening (EU) 2024/2847 van het Europees Parlement en de Raad

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) ([1]), en met name artikel 7, lid 4,

Overwegende hetgeen volgt:

(1) Verordening (EU) 2024/2847 bevat cyberbeveiligingsvereisten voor producten met digitale elementen. Bijlage III bij die verordening bevat met name categorieën belangrijke producten met digitale elementen die, als ze in de handel worden gebracht, onderworpen zijn aan conformiteitsbeoordelingsprocedures die strenger zijn dan de procedures die gelden voor andere producten met digitale elementen. Bijlage IV bij de verordening bevat categorieën kritieke producten met digitale elementen waarvoor van fabrikanten kan worden verlangd dat ze een Europees cyberbeveiligingscertificaat verkrijgen in het kader van een Europese cyberbeveiligingscertificeringsregeling overeenkomstig Verordening (EU) 2019/881 van het Europees Parlement en de Raad ([2]), of die onderworpen zijn aan een verplichte conformiteitsbeoordeling door derden als ze in de handel worden gebracht.

(2) Overeenkomstig artikel 7, lid 1, en artikel 8, lid 1, van Verordening (EU) 2024/2847 bepaalt de belangrijkste functionaliteit van een product met digitale elementen of dat product voldoet aan de technische beschrijving van een categorie belangrijke of kritieke producten met digitale elementen en dus aan de toepasselijke conformiteitsbeoordelingsprocedures.

(3) Bij de ontwikkeling van een product met digitale elementen en om over de gewenste functionaliteiten te beschikken, integreren fabrikanten in hun eigen producten met digitale elementen doorgaans andere componenten die ook producten met digitale elementen zijn en die kunnen voldoen aan de technische beschrijving van een categorie belangrijke of kritieke producten. Krachtens Verordening (EU) 2024/2847 is een product met digitale elementen onderworpen aan de conformiteitsbeoordelingsprocedures die gelden voor belangrijke of kritieke producten met digitale elementen als dat product als geheel een belangrijk of kritiek product is zoals bepaald in de bijlagen III en IV bij die verordening. De integratie van een ingebedde browser als onderdeel van een nieuwsapp voor gebruik in smartphones betekent op zich bijvoorbeeld niet dat de nieuwsapp onderworpen is aan de conformiteitsbeoordelingsprocedure die geldt voor producten met digitale elementen met als belangrijkste functionaliteit “op zichzelf staande en ingebedde browsers”. Niettemin moet de fabrikant er overeenkomstig Verordening (EU) 2024/2847 voor zorgen dat het product met digitale elementen als geheel aan de essentiële cyberbeveiligingsvereisten voldoet. Daarom moet de fabrikant de beveiliging van het gehele product evalueren en daarbij indien nodig rekening houden met de beveiliging van de componenten of functionaliteiten die erin zijn geïntegreerd. Om de fabrikant van een nieuwsapp bijvoorbeeld in staat te stellen om aan te tonen dat zijn product met digitale elementen voldoet aan Verordening (EU) 2024/2847, moet die fabrikant aantonen dat de nieuwsapp als geheel voldoet aan de toepasselijke vereisten en daarbij indien nodig rekening houden met de beveiliging van de ingebedde browser die in zijn app is geïntegreerd.

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

([2]) Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Dat een product met digitale elementen andere of extra functies vervult dan die beschreven in de technische beschrijvingen in deze verordening, betekent op zich niet dat het product met digitale elementen niet de belangrijkste functionaliteit heeft van een productcategorie zoals bepaald in de bijlagen III en IV bij Verordening (EU) 2024/2847. Producten met digitale elementen met als belangrijkste functionaliteit "besturingssystemen" bevatten bijvoorbeeld vaak software die ondersteunende functies vervult die niet in de technische beschrijving van die productcategorie zijn opgenomen, zoals rekenmachines of eenvoudige programma's voor grafische vormgeving. Producten met digitale elementen bevatten vaak ook componenten die de functionaliteit hebben van een ander belangrijk of kritiek product met digitale elementen, zoals een besturingssysteem waarin browserfunctionaliteiten geïntegreerd zijn, of een router waarin firewall-functionaliteiten geïntegreerd zijn. Dat betekent op zich echter niet dat dergelijke producten met digitale elementen niet als belangrijkste functionaliteit respectievelijk "besturingssystemen" of "routers, modems bestemd voor verbinding met het internet, en netwerkswitches" hebben.

(5) Anderzijds mag een product met digitale elementen dat de functies van een productcategorie zoals bepaald in de bijlagen III en IV bij Verordening (EU) 2024/2847 kan vervullen maar waarvan de belangrijkste functionaliteit zelf verschilt van die van een dergelijke productcategorie, niet worden geacht te voldoen aan de technische beschrijving van die productcategorie. Zo kan software voor beveiliging, automatisering en respons (SOAR) vaak de functies vervullen van producten met digitale elementen in de categorie "Security information and event management-systemen (SIEM) (beveiligingsinformatie en evenementenbeheer)", d.w.z. gegevens verzamelen, analyseren en presenteren als bruikbare informatie voor beveiligingsdoeleinden. Aangezien de belangrijkste functionaliteit echter niet die van een SIEM-systeem is, wordt SOAR-software over het algemeen niet geacht te voldoen aan de technische beschrijving van SIEM-systemen. Evenzo zijn in een smartphone doorgaans componenten geïntegreerd die de functies van verschillende productcategorieën zoals bepaald in de bijlagen III en IV bij Verordening (EU) 2024/2847 vervullen, zoals een besturingssysteem of een geïntegreerde wachtwoordbeheerder. Aangezien de belangrijkste functionaliteit van een smartphone echter niet die van een besturingssysteem of een wachtwoordbeheerder is, wordt die over het algemeen niet geacht te voldoen aan de technische beschrijving van dergelijke productcategorieën.

(6) Conform artikel 13, leden 2 en 3, van Verordening (EU) 2024/2847 moeten fabrikanten van producten met digitale elementen de essentiële cyberbeveiligingsvereisten van deel I van bijlage I bij Verordening (EU) 2024/2847 uitvoeren op een wijze die in verhouding staat tot de risico's van het product met digitale elementen, op basis van het beoogde doel en het redelijkerwijs voorzienbaar gebruik, alsook de voorwaarden van het gebruik, van het product met digitale elementen, waarbij rekening wordt gehouden met de verwachte gebruiksduur van het product. Overeenkomstig artikel 13, leden 2 en 3, van die verordening, en ongeacht of het product met digitale elementen wordt beschouwd als een belangrijk of kritiek product met digitale elementen, moeten fabrikanten een uitgebreide cyberbeveiligingsrisicobeoordeling uitvoeren en aangeven hoe de essentiële cyberbeveiligingsvereisten worden uitgevoerd op basis van de risicobeoordeling, inclusief het testen en waarborgen ervan. Als de belangrijkste functionaliteit van hun product met digitale elementen voldoet aan de technische beschrijving van een belangrijk of kritiek product met digitale elementen, moeten fabrikanten de conformiteit aantonen volgens de specifieke conformiteitsbeoordelingsprocedures die zijn vastgesteld in artikel 32, leden 2, 3, 4 en 5, van Verordening (EU) 2024/2847.

(7) Deze verordening bevat voorbeelden van producten met digitale elementen waarvan de belangrijkste functionaliteit voldoet aan de technische beschrijving van bepaalde belangrijke of kritieke producten met digitale elementen. Die voorbeelden worden louter ter illustratie gegeven en vormen geen uitputtende lijst.

(8) Om fabrikanten rechtszekerheid te bieden, moeten de producten met digitale elementen van de categorieën manipulatiebestendige microprocessoren, manipulatiebestendige microcontrollers en smartcards of soortgelijke apparaten, met inbegrip van secure elements (beveiligde elementen), worden onderscheiden op basis van de mate van weerstand tegen mogelijk misbruik van gebreken of zwakke punten waarvoor die zijn ontworpen. De AVA_VAN-niveaus zijn een veelgebruikte en gestandaardiseerde manier om een dergelijke weerstand uit te drukken. Ze zijn vastgelegd in de openbaar beschikbare normen voor gemeenschappelijke criteria en gemeenschappelijke evaluatiemethodologie, die bestaande certificeringskaders ondersteunen die breed toegepast worden op de markt, zoals Uitvoeringsverordening (EU) 2024/482 van de Commissie ([3]). Bij Uitvoeringsverordening (EU) 2024/482 is

([3]) Uitvoeringsverordening (EU) 2024/482 van de Commissie van 31 januari 2024 houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) (PB L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

een Europese cyberbeveiligingscertificeringsregeling vastgesteld die kan worden gebruikt om een product te certificeren op een specifiek zekerheidsniveau. Op basis van wereldwijde werkwijzen biedt Uitvoeringsverordening (EU) 2024/482 de mogelijkheid om tot eind 2027 certificaten af te geven op basis van oudere versies van de normen. In het licht van Verordening (EU) 2024/2847 is het dan ook passend dat de AVA_VAN-niveaus uitgedrukt mogen worden door te verwijzen naar de recentste of oudere versies van die normen.

(9) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 62, lid 1, van Verordening (EU) 2024/2847 ingestelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Definities

Voor de toepassing van deze verordening gelden de volgende definities:

1) "gemeenschappelijke criteria": de gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie in de zin van artikel 2, punt 1, van Uitvoeringsverordening (EU) 2024/482 of zoals vastgesteld in de in artikel 3, lid 2, punten a) en b), van die uitvoeringsverordening bedoelde normen;

2) "gemeenschappelijke evaluatiemethode": de gemeenschappelijke methodologie voor de evaluatie van de beveiliging van informatietechnologie in de zin van artikel 2, punt 2, van Uitvoeringsverordening (EU) 2024/482 of zoals vastgesteld in de in artikel 3, lid 2, punten c) en d), van die uitvoeringsverordening bedoelde normen.

Artikel 2

1. De technische beschrijving van de categorieën producten met digitale elementen van de klassen I en II van bijlage III bij Verordening (EU) 2024/2847 wordt opgenomen in bijlage I bij deze verordening.

2. De technische beschrijving van de categorieën producten met digitale elementen van bijlage IV bij Verordening (EU) 2024/2847 wordt opgenomen in bijlage II bij deze verordening.

Artikel 3

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 28 november 2025.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

BELANGRIJKE PRODUCTEN MET DIGITALE ELEMENTEN

Klasse I

Productcategorie	Technische beschrijving
1. Software en hardware voor identiteitsbeheersystemen en voor het beheer van geprivilegieerde toegang, met inbegrip van lezers voor authenticatie en toegangscontrole, waaronder biometrische lezers	Identiteitsbeheersystemen zijn producten met digitale elementen die mechanismen bevatten voor authenticatie of autorisatie en die ook mechanismen kunnen bevatten voor het beheer van de levenscyclus van identiteitsgegevens van natuurlijke personen, rechtspersonen, apparaten of systemen, zoals identiteitsregistratie, -voorziening, -onderhoud en -uitschrijving. Deze systemen omvatten toegangsbeheersystemen die de toegang van natuurlijke personen, rechtspersonen, apparaten of systemen tot digitale hulpmiddelen of fysieke locaties regelen. Software voor het beheer van geprivilegieerde toegang is een toegangsbeheersysteem dat de toegangsrechten tot IT- en OT-systemen en gevoelige informatie binnen een organisatie regelt en monitort, inclusief systemen die een gedifferentieerd toegangscontrolebeleid voor geprivilegieerde gebruikers handhaven. Deze categorie omvat, maar is niet beperkt tot, lezers voor authenticatie en toegangscontrole, biometrische lezers, software voor single sign-on, gefedereerde software voor identiteitsbeheer, software voor een eenmalig wachtwoord, hardware-authenticatieapparaten zoals generators voor transactie-authenticatienummers (TAN), authenticatiesoftware en multifactorauthenticatiesoftware.
2. Op zichzelf staande en ingebedde browsers	Softwareproducten met digitale elementen waarmee eindgebruikers toegang kunnen krijgen tot webcontent en -diensten die worden gehost op servers die verbonden zijn met netwerken zoals het internet, ze zichtbaar kunnen maken en ermee kunnen communiceren. Ze omvatten doorgaans een browser-engine voor de interpretatie en weergave van content die in markuptaal is geschreven (bv. HTML), ondersteuning voor webprotocollen (bv. HTTP, HTTPS), de mogelijkheid om scripts uit te voeren en gebruikersinput te beheren, en de opslag van tijdelijke of permanente gegevens van websites (cookies). Deze categorie omvat, maar is niet beperkt tot, op zichzelf staande toepassingen die de functies vervullen van browsers, ingebedde browsers die bedoeld zijn voor integratie in een ander systeem of een andere toepassing, en browsers met een geïntegreerde AI-agent.
3. Wachtwoordbeheerders (“Wachtwoordbeheer”)	Producten met digitale elementen die wachtwoorden opslaan (lokaal op een apparaat of op afstand op een server), waaronder activiteiten zoals het genereren en delen wachtwoorden en de integratie met lokale toepassingen of toepassingen van derden voor het gebruik van wachtwoorden. Deze categorie omvat, maar is niet beperkt tot, lokale, bedrijfs- en hardware-wachtwoordbeheerders en wachtwoordbeheerders die als browserextensies aangeboden worden.

Productcategorie	Technische beschrijving
4. Software die kwaadaardige software opzoekt, verwijdert of in quarantaine plaatst	Softwareproducten met digitale elementen, doorgaans antivirus- of antimalware genoemd, die kwaadaardige software of code op apparaten detecteren, zoeken, verwijderen of in quarantaine plaatsen om de integriteit, vertrouwelijkheid of beschikbaarheid van de apparaten te handhaven. Binnen deze productcategorie wordt onder “kwaadaardige software” software verstaan met kwaadaardige kenmerken of vermogens die direct of indirect schade kunnen toebrengen aan de gebruiker en/of het computersysteem, zoals virussen, wormen, ransomware, spyware en Trojaanse paarden. Deze categorie omvat, maar is niet beperkt tot, software die kwaadaardige software in realtime of handmatig detecteert of zoekt, rootkitdetectie en reddingsdisks met als belangrijkste functionaliteit het zoeken, verwijderen of in quarantaine plaatsen van kwaadaardige software.
5. Producten met digitale elementen met de functie van virtueel particulier netwerk (VPN)	Producten met digitale elementen die een versleutelde logische tunnel tot stand brengen die is opgebouwd uit de systeembronnen van een fysiek of virtueel netwerk. Deze categorie omvat, maar is niet beperkt tot, clients, servers en gateways van virtuele particuliere netwerken.
6. Netwerkbeheersystemen	Producten met digitale elementen die verbonden netwerkelementen beheren, zoals servers, routers, netwerkswitches, werkstations, printers en mobiele apparaten, door die te monitoren en hun netwerkwerking en -configuratie te regelen. Deze categorie omvat, maar is niet beperkt tot, end-to-endbeheersystemen en specifieke configuratiebeheersystemen, zoals controllers voor softwaregedefinieerde netwerken.
7. Security information and event management-systemen (SIEM) (beveiligingsinformatie en evenementenbeheer)	Producten met digitale elementen die gegevens uit meerdere bronnen verzamelen, analyseren, correleren en presenteren als bruikbare informatie voor veiligheidsdoeleinden, zoals de opsporing van dreigingen en incidenten, forensisch onderzoek of nalevingsdoeleinden.
8. Bootmanagement	Softwareproducten met digitale elementen die het proces van de initiële start van het systeem beheren na opstart/herstart door hardware te initialiseren, de besturing te laden of de controle over te dragen aan de besturingssysteemomgeving of de systeembronnen, en startopties te selecteren. Deze categorie omvat, maar is niet beperkt tot, UEFI-firmware en eenfase- en meerfasenopstartladers.
9. Publiekesleutelinfrastructuur en software voor de afgifte van digitale certificaten	Producten met digitale elementen die worden gebruikt als onderdeel van een publiekesleutelinfrastructuur (PKI) en de validering, creatie, afgifte, distributie, statuspublicatie, vernieuwing of intrekking van digitale certificaten of de generatie, opslag, escrow, uitwisseling, vernietiging of doorgave van cryptografische sleutels die verband houden met dergelijke digitale certificaten beheren. Deze categorie omvat, maar is niet beperkt tot, sleutelbeheerssystemen, digitale systemen voor certificaatbeheer, OCSP-responders (Online Certificate Status Protocol) en all-in-one PKI-oplossingen.

Productcategorie	Technische beschrijving
10. Fysieke en virtuele netwerkinterfaces	Fysieke netwerkinterfaces zijn producten met digitale elementen die een apparaat rechtstreeks met een netwerk verbinden via een applicatieprogramma-interface (API) die wordt geleverd door de interface-stuurprogramma's die doorgaans op de datalinklaag werken, en die voorzien zijn van hardware-adapters voor transmissiemedia met overeenkomstige firmware die doorgaans op de fysieke en de datalinklaag werkt. Virtuele netwerkinterfaces zijn producten met digitale elementen die een apparaat rechtstreeks of onrechtstreeks verbinden met een netwerk via een API die die van bestuurders van fysieke netwerkinterfaces die doorgaans op de datalinklaag werken, simuleert. Deze categorie omvat, maar is niet beperkt tot, bedrade en draadloze netwerkinterfacekaarten, controllers en adapters, zoals voor wifi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee of Fieldbus, en ook louter virtuele, op zichzelf staande producten, zoals virtuele netwerkinterfacekaarten, containernetwerkinterfaces en VPN-interfaces.
11. Besturingssystemen	Softwareproducten met digitale elementen die een abstracte interface van de onderliggende hardware bieden en de uitvoering van software regelen, en die diensten kunnen verlenen zoals computermiddelenbeheer en -configuratie, planning, input-outputbeheer, gegevensbeheer en een interface waarlangs toepassingen interageren met systeemmiddelen en randapparatuur. Deze categorie omvat, maar is niet beperkt tot, realtime-besturingssystemen en besturingssystemen voor algemene en voor speciale doeleinden.
12. Routers, modems bestemd voor verbinding met het internet, en netwerkswitches	Routers zijn producten met digitale elementen die de gegevensstroom tussen verschillende netwerken tot stand brengen en regelen door paden of routes te kiezen met behulp van routeringsprotocolmechanismen en algoritmen die doorgaans op de netwerklaag werken. Deze categorie omvat, maar is niet beperkt tot, bedrade en draadloze routers, virtuele routers en routers met of zonder modems.
	Modems bestemd voor verbinding met het internet zijn hardwareproducten met digitale elementen die gebruikmaken van digitale modulatie- en demodulatietechnieken om analoge signalen om te zetten van en naar digitale signalen voor IP-communicatie. Deze categorie omvat onder meer glasvezel-, DSL- (Digital Subscriber Line), kabel- (DOCSIS), satelliet- en cellulaire modems.
	Netwerkswitches zijn producten met digitale elementen die verbinding leggen tussen genetwerkte apparaten via pakkettransportmechanismen en die een beheerslaag hebben, doorgaans op de datalink- of de netwerklaag. Deze categorie omvat, maar is niet beperkt tot, beheers-, slimme en meerlagige switches, virtuele beveiligingsswitches, programmeerbare switches voor softwaregedefinieerde netwerken en bruggen zoals draadloze toegangspunten.

Productcategorie	Technische beschrijving
13. Microprocessoren met beveiligingsgerelateerde functies	Producten met digitale elementen die geïntegreerde schakelingen zijn die centrale verwerkingsfuncties uitvoeren op basis van extern geheugen en randapparatuur, waaronder microcode en andere eenvoudige firmware. Daarnaast bieden ze beveiligingsgerelateerde functies, zoals versleuteling, authenticatie, veilige sleutelopslag, willekeurige nummergeneratie, betrouwbare uitvoeringsomgevingen of andere op hardware gebaseerde beschermingsmechanismen, om andere producten, netwerken of diensten te beveiligen buiten de microprocessor zelf, zoals een beveiligde opstartketen, virtualisatie of beveiligde communicatie-interfaces.
14. Microcontrollers met beveiligingsgerelateerde functies	Producten met digitale elementen die geïntegreerde schakelingen zijn die centrale verwerkingsfuncties uitvoeren met integratie van het geheugen, waardoor de microcontroller en doorgaans ook andere randapparatuur (zoals microcode en andere eenvoudige firmware) programmeerbaar worden. Daarnaast bieden ze beveiligingsgerelateerde functies, zoals versleuteling, authenticatie, veilige sleutelopslag, willekeurige nummergeneratie, betrouwbare uitvoeringsomgevingen of andere op hardware gebaseerde beschermingsmechanismen, om andere producten, netwerken of diensten te beveiligen buiten de microcontrollers zelf, zoals een beveiligde opstartketen, virtualisatie of beveiligde communicatie-interfaces.
15. Toepassingsspecifieke geïntegreerde schakelingen (ASIC) en veld-programmeerbare gatearrays (FPGA) met beveiligingsgerelateerde functies	ASIC met beveiligingsgerelateerde functies zijn producten met digitale elementen die geïntegreerde schakelingen zijn die geheel of gedeeltelijk op maat zijn ontworpen om een specifieke functie te vervullen of een specifieke toepassing uit te voeren, zoals microcode en andere eenvoudige firmware. Daarnaast bieden ze beveiligingsgerelateerde functies, zoals versleuteling, authenticatie, veilige sleutelopslag, willekeurige nummergeneratie, betrouwbare uitvoeringsomgevingen of andere op hardware gebaseerde beschermingsmechanismen, om andere producten, netwerken of diensten te beveiligen buiten de ASIC zelf, zoals een beveiligde opstartketen, virtualisatie of beveiligde communicatie-interfaces.
	FPGA met beveiligingsgerelateerde functies zijn producten met digitale elementen die geïntegreerde schakelingen zijn en worden gekenmerkt door een matrix van configureerbare logische blokken die zijn ontworpen om na fabricage herprogrammeerbaar te zijn om een specifieke functie te vervullen of een specifieke toepassing uit te voeren, zoals microcode en andere eenvoudige firmware. Daarnaast bieden ze beveiligingsfuncties, zoals versleuteling, authenticatie, veilige sleutelopslag, willekeurige nummergeneratie, betrouwbare uitvoeringsomgevingen of andere op hardware gebaseerde beschermingsmechanismen, om andere producten, netwerken of diensten te beveiligen buiten de FPGA zelf, zoals een beveiligde opstartketen, virtualisatie of beveiligde communicatie-interfaces.
16. Virtuele assistenten voor slimme huizen voor algemene doeleinden	Producten met digitale elementen die rechtstreeks of via andere apparatuur op het openbare internet communiceren en die behoeften, taken of vragen op basis van natuurlijke taal vereisen, zoals audio- of schriftelijke input, en die op basis van die behoeften, taken of vragen toegang bieden tot andere diensten of de functies van verbonden apparaten in residentiële instellingen regelen. Deze categorie omvat, maar is niet beperkt tot, slimme luidsprekers met een geïntegreerde virtuele assistent, en op zichzelf staande virtuele assistenten die aan deze beschrijving voldoen.

Productcategorie	Technische beschrijving
17. Producten voor slimme huizen met beveiligingsfuncties, met inbegrip van slimme deursloten, beveiligingscamera's, babymonitoringsystemen en alarmsystemen	Producten met digitale elementen die de fysieke veiligheid van consumenten in een residentiële omgeving beschermen en op afstand vanuit andere systemen geregeld of beheerd kunnen worden, alsook hardware en software die dergelijke producten centraal beheren. Deze categorie omvat, maar is niet beperkt tot, slimme deurvergrendelingen, babymonitoringsystemen, alarmsystemen en beveiligingscamera's voor woningen.
18. Met het internet verbonden speelgoed dat onder Richtlijn 2009/48/EG van het Europees Parlement en de Raad ([1]) valt en sociale interactieve functies (bv. spreken of filmen) of locatietraceringsfuncties heeft	Met internet verbonden speelgoed dat sociale interactieve functies heeft, zijn producten met digitale elementen die onder Richtlijn 2009/48/EG vallen, rechtstreeks of via andere apparatuur op het openbare internet communiceren en ingebedde technologie bevatten die inkomende en uitgaande communicatie mogelijk maken, zoals een toetsenbord, microfoon, luidspreker of camera.
	Met internet verbonden speelgoed dat locatietraceringsfuncties heeft, zijn producten met digitale elementen die onder Richtlijn 2009/48/EG vallen, rechtstreeks of via andere apparatuur op openbare internet communiceren en technologie bevatten waarmee de geografische locatie van het speelgoed of de gebruiker ervan kan worden gevolgd of afgeleid. Als het speelgoed alleen de nabijheid van de gebruiker of ander speelgoed detecteert met behulp van detectietechnologie, wordt het speelgoed niet geacht locatietraceringsfuncties te hebben.
19. Persoonlijke wearables die op een menselijk lichaam moeten worden gedragen of geplaatst en bedoeld zijn voor gezondheidsmonitoring (zoals tracking) en die niet onder Verordening (EU) 2017/745 ([2]) of (EU) 2017/746 van het Europees Parlement en de Raad ([3]) vallen, of persoonlijke wearables die bestemd zijn voor gebruik door en voor kinderen	Persoonlijke wearables die op een menselijk lichaam moeten worden gedragen of geplaatst en bedoeld zijn voor gezondheidsmonitoring, zijn producten met digitale elementen die rechtstreeks of via kleding of accessoires op het lichaam worden gedragen en die regelmatig of voortdurend informatie, waaronder lichaamsgegevens, kunnen verwerken met betrekking tot de gezondheid van de gebruiker, met uitzondering van producten die binnen het toepassingsgebied van Verordening (EU) 2017/745 of Verordening (EU) 2017/746 vallen. Deze categorie omvat, maar is niet beperkt tot, fitnesstrackers, smartwatches, slimme juwelen, slimme kleding en sportkleding die aan deze beschrijving voldoen.
	Persoonlijke wearables die bestemd zijn voor gebruik door en voor kinderen zijn producten met digitale elementen die rechtstreeks of via kleding of accessoires op het lichaam kunnen worden gedragen of geplaatst van personen jonger dan 14 jaar. Deze categorie omvat, maar is niet beperkt tot, wearables voor kinderveiligheid.

([1]) Richtlijn 2009/48/EG van het Europees Parlement en de Raad van 18 juni 2009 betreffende de veiligheid van speelgoed (PB L 170 van 30.6.2009, blz. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad (PB L 117 van 5.5.2017, blz. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek en tot intrekking van Richtlijn 98/79/EG en Besluit 2010/227/EU van de Commissie (PB L 117 van 5.5.2017, blz. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Klasse II

Productcategorie	Technische beschrijving
1. Hypervisors en containerruntimesystemen die de gevirtualiseerde uitvoering van besturingssystemen en soortgelijke omgevingen ondersteunen	Hypervisors zijn softwareproducten met digitale elementen die computermiddelen onttrekken en/of toewijzen en de uitvoering, het beheer en de orkestratie van virtuele machines mogelijk maken die logisch van elkaar en/of van de fysieke hardware gescheiden zijn. Hypervisors kunnen rechtstreeks werken op hardware (onbedekt metaal), op een besturingssysteem of in een andere virtuele machine (ingebedde virtualisatie). Binnen deze productcategorie wordt onder “virtuele machine” een softwaregedefinieerde logische scheiding van een computeromgeving verstaan die een gevirtualiseerde reeks hardware-middelen (bv. CPU, geheugen, opslag, netwerkinterfaces) omvat en gewoonlijk een eigen besturingssysteem host. Deze categorie omvat, maar is niet beperkt tot, hypervisors van type 1 (onbedekt metaal), hypervisors van type 2 (gehost op een besturingssysteem) en hybride hypervisors.
	Containerruntimesystemen zijn softwareproducten met digitale elementen die de uitvoering en levenscyclus van containers beheren die op één enkel hostbesturingssysteem lopen als geïsoleerde processen, middelen toewijzen en het beheer en de orkestratie van individuele containers mogelijk maken. Binnen deze productcategorie wordt onder “container” een op software gebaseerde uitvoeringsomgeving verstaan waaronder een of meer softwarecomponenten en de afhankelijkheden ervan in één pakket vallen, zodat hij onafhankelijk en consistent kan werken.
2. Firewalls, inbraakdetectiesystemen en inbraakpreventiesystemen	Firewalls zijn producten met digitale elementen die een verbonden netwerk of systeem tegen ongeoorloofde toegang beschermen door het datacommunicatieverkeer van en naar dat netwerk te monitoren en te beperken. Deze categorie omvat, maar is niet beperkt tot, firewalls voor netwerken en toepassingen, zoals firewalls of filters voor webtoepassingen en antispam-gateways.
	Inbraakdetectiesystemen zijn producten met digitale elementen die het verkeer op verdachte activiteiten monitoren nadat het in de netwerkomgeving terechtkomt en die detecteren of vaststellen dat een inbraak heeft plaatsgevonden, plaatsvindt of heeft plaatsgevonden op een verbonden netwerk of systeem. Deze categorie omvat, maar is niet beperkt tot, netwerk- en host-gebaseerde inbraakdetectiesystemen.
	Inbraakpreventiesystemen zijn producten met digitale elementen die bestaan uit een inbraakdetectiesysteem dat actief reageert op een inbraak op een verbonden netwerk of systeem. Deze categorie omvat, maar is niet beperkt tot, netwerk- en host-gebaseerde inbraakpreventiesystemen.

Productcategorie	Technische beschrijving
3. Manipulatiebestendige microprocessoren	Producten met digitale elementen die microprocessoren zijn met beveiligingsgerelateerde functies als bedoeld in tabel "Klasse I", punt 13, van deze bijlage, inclusief bewijs van manipulatie, weerstand of reactie, en die bovendien zijn ontworpen om een beschermingsniveau van AVA_VAN 2 of 3 te bieden, zoals bepaald in de gemeenschappelijke criteria en de gemeenschappelijke evaluatiemethode.
4. Manipulatiebestendige microcontrollers	Producten met digitale elementen die microcontrollers zijn met beveiligingsgerelateerde functies als bedoeld in tabel "Klasse I", punt 14, van deze bijlage, inclusief bewijs van manipulatie, weerstand of reactie, en die bovendien zijn ontworpen om een beschermingsniveau van AVA_VAN 2 of 3 te bieden, zoals bepaald in de gemeenschappelijke criteria en de gemeenschappelijke evaluatiemethode.

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

BIJLAGE II

KRITIEKE PRODUCTEN MET DIGITALE ELEMENTEN

Productcategorie	Technische beschrijving
1. Hardwareapparaten met beveiligingskastje	Hardwareproducten met digitale elementen die gevoelige gegevens veilig opslaan, verwerken of beheren of cryptografische bewerkingen uitvoeren, en die bestaan uit meerdere afzonderlijke componenten, met een fysieke hardware-enveloppe die bewijs van manipulatie, weerstand of reactie biedt als tegenmaatregelen tegen fysieke aanvallen. Deze categorie omvat, maar is niet beperkt tot, fysieke betaalterminals, hardware-beveiligingsmodules die cryptografische elementen genereren en beheren, en tachografen die aan de bovenstaande beschrijving voldoen.
2. Gateways voor slimme meters binnen slimme-metersystemen zoals gedefinieerd in artikel 2, punt 23, van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad ([1]) en andere apparaten voor geavanceerde beveiligingsdoeleinden, onder meer voor beveiligde cryptoverwerking	Gateways voor slimme meters zijn producten met digitale elementen die de communicatie regelen tussen componenten in of verbonden met slimme-metersystemen zoals gedefinieerd in artikel 2, punt 23, van Richtlijn (EU) 2019/944, en gemachtigde derden, zoals nutsbedrijven. Dergelijke gateways verzamelen, verwerken en slaan meter- of persoonsgegevens op, beschermen gegevens- en informatiestromen door specifieke cryptografische behoeften (zoals versleuteling en ontsleuteling van gegevens) te ondersteunen, incorporeren firewall-functionaliteiten en bieden de middelen om andere apparaten te beheren. Deze categorie omvat, maar is niet beperkt tot, gateways voor slimme meters met betrekking tot slimme-metersystemen die elektriciteit meten zoals gedefinieerd in artikel 2, punt 23, van Richtlijn (EU) 2019/944. Ze kan ook gateways voor slimme meters omvatten die worden gebruikt in andere slimme-metersystemen die het verbruik van andere energiebronnen meten, zoals gas of warmte, mits de gateway aan deze beschrijving voldoet.
3. Smartcards of soortgelijke apparaten, met inbegrip van secure elements (beveiligde elementen)	Beveiligde elementen zijn microcontrollers of microprocessoren met beveiligingsgerelateerde functies, waaronder bewijs van manipulatie, weerstand of respons. Doorgaans bewaren, verwerken of beheren ze cryptografische acties of gevoelige gegevens, zoals identiteits- of betalingsgegevens. Beveiligde elementen zijn ontworpen om minstens een beschermingsniveau van AVA_VAN.4 te bieden, zoals uiteengezet in de gemeenschappelijke criteria of de gemeenschappelijke evaluatiemethode. Ze kunnen op zichzelf staand silicium zijn of kunnen worden geïntegreerd in systemen-op-chip (SoC). Beveiligde elementen kunnen een toepassingsomgeving of een besturingssysteem incorporeren en een of meer toepassingen omvatten. Deze categorie omvat, maar is niet beperkt tot, Trusted Platform Modules (TPM's) en ingebedde Universal Integrated Circuit Cards (UICC's).
	Smartcards of soortgelijke apparaten zijn beveiligde elementen die in een dragermateriaal zijn geïntegreerd, zoals plastic of hout, in de vorm van een kaart, of beveiligde elementen die in dragermaterialen zijn geïntegreerd en andere vormen aannemen. Deze categorie omvat, maar is niet beperkt tot, identiteits- en reisdocumenten, gekwalificeerde handtekeningkaarten, vervangbare UICC's, fysieke betaal- en toegangskaarten, digitale tachograafkaarten of polsbanden met geïntegreerde beveiligde betaalelementen.

([1]) Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (PB L 158 van 14.6.2019, blz. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).