Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/2392

1.12.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/2392

z dnia 28 listopada 2025 r.

w sprawie opisu technicznego kategorii ważnych i krytycznych produktów z elementami cyfrowymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/2847

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) ([1]), w szczególności jego art. 7 ust. 4,

a także mając na uwadze, co następuje:

(1) W rozporządzeniu (UE) 2024/2847 określono zasady dotyczące cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi. W szczególności w załączniku III do tego rozporządzenia określono kategorie ważnych produktów z elementami cyfrowymi, które po wprowadzeniu do obrotu podlegają bardziej rygorystycznym procedurom oceny zgodności niż procedury mające zastosowanie do innych produktów z elementami cyfrowymi. W załączniku IV do rozporządzenia (UE) 2024/2847 określono kategorie krytycznych produktów z elementami cyfrowymi, w przypadku których producenci mogliby być zobowiązani do uzyskania europejskiego certyfikatu cyberbezpieczeństwa w ramach europejskiego programu certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 ([2]) lub które podlegałyby obowiązkowej ocenie zgodności przez stronę trzecią w momencie wprowadzenia do obrotu.

(2) Zgodnie z art. 7 ust. 1 i art. 8 ust. 1 rozporządzenia (UE) 2024/2847 podstawowa funkcjonalność produktu z elementami cyfrowymi decyduje o tym, czy ten produkt z elementami cyfrowymi odpowiada opisowi technicznemu kategorii ważnych lub krytycznych produktów z elementami cyfrowymi, a tym samym podlega procedurom oceny zgodności mającym do nich zastosowanie.

(3) Opracowując produkt z elementami cyfrowymi, aby osiągnąć pożądany zestaw funkcji, producenci zazwyczaj włączają do swoich własnych produktów z elementami cyfrowymi inne komponenty, które również stanowią produkty z elementami cyfrowymi i które mogą odpowiadać opisowi technicznemu kategorii ważnych lub krytycznych produktów. Zgodnie z rozporządzeniem (UE) 2024/2847 produkt z elementami cyfrowymi podlega procedurom oceny zgodności mającym zastosowanie do ważnych lub krytycznych produktów z elementami cyfrowymi, jeżeli produkt ten jako całość jest ważnym lub krytycznym produktem, jak określono w załącznikach III i IV do tego rozporządzenia. Na przykład włączenie wbudowanej przeglądarki jako komponentu aplikacji informacyjnej do użytku w smartfonach nie sprawia samo w sobie, że aplikacja informacyjna podlega procedurze oceny zgodności mającej zastosowanie do produktów z elementami cyfrowymi, których podstawowa funkcjonalność to „samodzielne i wbudowane przeglądarki". Zgodnie z rozporządzeniem (UE) 2024/2847 producent musi jednak zapewnić, aby produkt z elementami cyfrowymi jako całość spełniał zasadnicze wymagania w zakresie cyberbezpieczeństwa. W związku z tym producent musi ocenić bezpieczeństwo całego produktu, uwzględniając, w stosownych przypadkach, bezpieczeństwo włączonych do niego komponentów lub funkcji. Na przykład, aby producent aplikacji informacyjnej mógł wykazać, że jego produkt z elementami cyfrowymi jest zgodny z rozporządzeniem (UE) 2024/2847, ma on wykazać, że aplikacja informacyjna jako całość spełnia mające zastosowanie wymogi, biorąc pod uwagę, w stosownych przypadkach, bezpieczeństwo wbudowanej przeglądarki, która została włączona do aplikacji.

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

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Fakt, że produkt z elementami cyfrowymi pełni funkcje inne lub dodatkowe w stosunku do funkcji określonych w opisach technicznych zawartych w niniejszym rozporządzeniu, nie oznacza sam w sobie, że produkt z elementami cyfrowymi nie posiada podstawowej funkcjonalności kategorii produktu określonej w załącznikach III i IV do rozporządzenia (UE) 2024/2847. Na przykład produkty z elementami cyfrowymi, których podstawowa funkcjonalność to „systemy operacyjne", często obejmują oprogramowanie, które pełni funkcje pomocnicze nieuwzględnione w opisie technicznym tej kategorii produktów, takie jak kalkulatory lub proste programy do obróbki graficznej. Produkty z elementami cyfrowymi często zawierają również komponenty, które posiadają funkcjonalność innego ważnego lub krytycznego produktu z elementami cyfrowymi, takie jak system operacyjny z wbudowaną funkcją przeglądarki lub router z wbudowaną funkcją zapory sieciowej. Nie oznacza to jednak, że takie produkty z elementami cyfrowymi nie mają podstawowej funkcjonalności, odpowiednio, „systemów operacyjnych" lub „routerów, modemów przeznaczonych do podłączenia do internetu i przełączników".

(5) Z drugiej strony produkt z elementami cyfrowymi, który może pełnić funkcje kategorii produktu określonej w załącznikach III i IV do rozporządzenia (UE) 2024/2847, ale którego podstawowa funkcjonalność sama w sobie różni się od podstawowej funkcjonalności takiej kategorii produktu, nie powinien być uznawany za odpowiadający opisowi technicznemu tej kategorii produktu. Na przykład oprogramowanie do orkiestracji, automatyzacji i reagowania na incydenty bezpieczeństwa (SOAR) często ma zdolność do pełnienia funkcji produktów z elementami cyfrowymi w kategorii „systemy zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM)", takich jak gromadzenie danych, ich analizowanie i prezentowanie jako informacji możliwych do zastosowania do celów bezpieczeństwa. Ponieważ jednak podstawową funkcjonalnością oprogramowania SOAR nie jest funkcja SIEM, zasadniczo nie należy tego oprogramowania uznawać za odpowiadające opisowi technicznemu „systemów zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM)". Podobnie smartfon zazwyczaj ma wbudowane komponenty, które pełnią funkcje kilku kategorii produktów określonych w załącznikach III i IV do rozporządzenia (UE) 2024/2847, takie jak system operacyjny lub zintegrowany menedżer haseł. Ponieważ jednak podstawową funkcjonalnością smartfona nie jest system operacyjny ani menedżer haseł, zasadniczo nie należy go uznawać za odpowiadający opisowi technicznemu takich kategorii produktów.

(6) Zgodnie z art. 13 ust. 2 i 3 rozporządzenia (UE) 2024/2847 producenci produktów z elementami cyfrowymi mają wdrożyć zasadnicze wymagania w zakresie cyberbezpieczeństwa określone w części I załącznika I do rozporządzenia (UE) 2024/2847 w sposób proporcjonalny do ryzyka związanego z produktem z elementami cyfrowymi, w oparciu o przeznaczenie i racjonalnie przewidywalne wykorzystanie, a także warunki korzystania z produktu z elementami cyfrowymi, z uwzględnieniem oczekiwanego czasu użytkowania produktu. Zgodnie z art. 13 ust. 2 i 3 tego rozporządzenia i niezależnie od tego, czy produkt z elementami cyfrowymi uznaje się za ważny lub krytyczny produkt z elementami cyfrowymi, producenci mają przeprowadzić kompleksową ocenę ryzyka w cyberprzestrzeni i wskazać, w jaki sposób wdrażane są zasadnicze wymagania w zakresie cyberbezpieczeństwa w oparciu o ocenę ryzyka, w tym na etapie testowania i zabezpieczania produktów. W przypadku gdy podstawowa funkcjonalność produktu z elementami cyfrowymi odpowiada opisowi technicznemu ważnego lub krytycznego produktu z elementami cyfrowymi, producenci muszą wykazać zgodność ze szczegółowymi procedurami oceny zgodności ustanowionymi w art. 32 ust. 2, 3, 4 i 5 rozporządzenia (UE) 2024/2847.

(7) W niniejszym rozporządzeniu zawarto przykłady produktów z elementami cyfrowymi, których podstawowa funkcjonalność odpowiada opisowi technicznemu niektórych ważnych lub krytycznych produktów z elementami cyfrowymi. Przykłady te podano wyłącznie w celach poglądowych i nie stanowią one wyczerpującego wykazu.

(8) Aby zagwarantować pewność prawa producentom, należy rozróżnić kategorie produktów z elementami cyfrowymi, które są mikroprocesorami odpornymi na manipulacje, mikrokontrolerami odpornymi na manipulacje oraz kartami elektronicznymi i podobnymi urządzeniami, w tym elementami zabezpieczającymi, na podstawie poziomu odporności na potencjalne wykorzystanie wad lub słabości, w odpowiedzi na które zostały zaprojektowane. Poziom AVA_VAN jest powszechnie stosowanym i znormalizowanym sposobem wyrażania takiego poziomu odporności. Poziomy AVA_VAN określono w publicznie dostępnych normach *Common Criteria* (wspólne kryteria) i *Common Evaluation Methodology* (wspólna metodyka oceny), które leżą u podstaw obecnie stosowanych ram certyfikacji powszechnie przyjętych na rynku, takich jak rozporządzenie wykonawcze Komisji (UE) 2024/482 ([3]).

([3]) Rozporządzenie wykonawcze Komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) (Dz.U. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

W rozporządzeniu wykonawczym (UE) 2024/482 ustanowiono europejski program certyfikacji cyberbezpieczeństwa, z którego można korzystać do celów certyfikacji produktu na określonym poziomie uzasadnienia zaufania. W oparciu o stosowane na świecie praktyki w rozporządzeniu wykonawczym (UE) 2024/482 przewidziano możliwość wydawania certyfikatów opartych na starszych wersjach norm do końca 2027 r. W związku z tym w kontekście rozporządzenia (UE) 2024/2847 należy dopuścić możliwość wyrażania poziomów AVA_VAN poprzez odniesienie albo do najnowszej wersji albo do starszych wersji tych standardów.

(9) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego w art. 62 ust. 1 rozporządzenia (UE) 2024/2847,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „wspólne kryteria" oznaczają wspólne kryteria oceny bezpieczeństwa technologii informacyjnych zdefiniowane w art. 2 pkt 1 rozporządzenia wykonawczego (UE) 2024/482 lub określone w normach, o których mowa w art. 3 ust. 2 lit. a) i b) tego rozporządzenia wykonawczego;

2) „wspólna metodyka oceny" oznacza wspólną metodykę oceny bezpieczeństwa technologii informacyjnych zdefiniowaną w art. 2 pkt 2 rozporządzenia wykonawczego (UE) 2024/482 lub określoną w normach, o których mowa w art. 3 ust. 2 lit. c) i d) tego rozporządzenia wykonawczego.

Artykuł 2

1. Opis techniczny kategorii produktów z elementami cyfrowymi należących do klas I i II wymienionych w załączniku III do rozporządzenia (UE) 2024/2847 określono w załączniku I do niniejszego rozporządzenia.

2. Opis techniczny kategorii produktów z elementami cyfrowymi wymienionych w załączniku IV do rozporządzenia (UE) 2024/2847 określono w załączniku II do niniejszego rozporządzenia.

Artykuł 3

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 28 listopada 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

WAŻNE PRODUKTY Z ELEMENTAMI CYFROWYMI

Klasa I

Kategoria produktów	Opis techniczny
1. Oprogramowanie systemów zarządzania tożsamością i zarządzania uprzywilejowanym dostępem oraz odpowiedni sprzęt, w tym czytniki do uwierzytelniania i kontroli dostępu, także biometryczne	Systemy zarządzania tożsamością to produkty z elementami cyfrowymi, które zapewniają mechanizmy uwierzytelniania lub autoryzacji i które mogą również zapewniać mechanizmy zarządzania cyklem życia poświadczeń tożsamości osób fizycznych, osób prawnych, urządzeń lub systemów, takie jak rejestracja tożsamości, konfigurowanie dostępu, utrzymanie poświadczenia tożsamości, wyrejestrowanie. Systemy te obejmują systemy zarządzania dostępem, które kontrolują dostęp osób fizycznych, osób prawnych, urządzeń lub systemów do zasobów cyfrowych lub fizycznych lokalizacji. Oprogramowanie systemów zarządzania uprzywilejowanym dostępem to system zarządzania dostępem, który kontroluje i monitoruje prawa dostępu do systemów IT (technologii informacyjnych) lub systemów OT (technologii operacyjnych) oraz do informacji szczególnie chronionych w ramach organizacji, co obejmuje systemy egzekwujące odmienne polityki kontroli dostępu dla użytkowników uprzywilejowanych. Kategoria ta obejmuje m.in. czytniki do uwierzytelniania i kontroli dostępu, czytniki biometryczne, oprogramowanie Single Sign-On (SSO, mechanizm jednokrotnego logowania), sfederowane oprogramowanie do zarządzania tożsamością, oprogramowanie do generowania i weryfikacji haseł jednorazowych, sprzętowe urządzenia uwierzytelniające, takie jak generatory kodów do uwierzytelniania transakcji (TAN), oprogramowanie uwierzytelniające i oprogramowanie do uwierzytelniania wieloskładnikowego.
2. Samodzielne i wbudowane przeglądarki	Oprogramowanie z elementami cyfrowymi, które umożliwia użytkownikom końcowym dostęp do treści i usług internetowych hostowanych na serwerach, które są podłączone do sieci, takich jak internet, oraz umożliwia im wyświetlanie tych treści i usług oraz interakcję z nimi. Zazwyczaj obejmuje silnik przeglądarki do interpretowania i wyświetlania treści zapisanych w języku znaczników (np. HTML), obsługę protokołów internetowych (np. HTTP, HTTPS), zdolność do wykonywania skryptów i zarządzania danymi wprowadzanymi przez użytkowników, a także przechowywanie tymczasowych lub trwałych danych ze stron internetowych (pliki cookie). Kategoria ta obejmuje m.in. samodzielne aplikacje pełniące funkcje przeglądarek, wbudowane przeglądarki przeznaczone do integracji z innym systemem lub inną aplikacją, a także przeglądarki z integracją agenta sztucznej inteligencji.
3. Menedżery haseł	Produkty z elementami cyfrowymi, które przechowują hasła, lokalnie na urządzeniu lub na zdalnym serwerze, a także umożliwiają czynności takie jak generowanie haseł i udostępnianie haseł oraz integrację z lokalnymi aplikacjami lub aplikacjami zewnętrznymi na potrzeby korzystania z haseł. Kategoria ta obejmuje m.in. lokalne menedżery haseł, menedżery haseł udostępniane jako rozszerzenia przeglądarki, firmowe menedżery haseł, a także sprzętowe menedżery haseł.

Kategoria produktów	Opis techniczny
4. Oprogramowanie, które wyszukuje, usuwa lub poddaje kwarantannie złośliwe oprogramowanie	Oprogramowanie z elementami cyfrowymi, nazywane zwykle oprogramowaniem antywirusowym lub oprogramowaniem *antimalware*, które wykrywa lub wyszukuje na urządzeniach złośliwe oprogramowanie lub złośliwy kod i usuwa takie oprogramowanie lub taki kod lub poddaje je kwarantannie w celu zachowania integralności, poufności lub dostępności wspomnianych urządzeń. W kontekście tej kategorii produktów „złośliwe oprogramowanie" oznacza oprogramowanie zawierające szkodliwe funkcje lub zdolności, które mogą wyrządzić bezpośrednią lub pośrednią szkodę użytkownikowi lub systemowi komputerowemu, takie jak wirusy, robaki, oprogramowanie szantażujące, oprogramowanie szpiegujące i trojany. Kategoria ta obejmuje m.in. oprogramowanie, które wykrywa lub wyszukuje złośliwe oprogramowanie w czasie rzeczywistym lub na polecenie użytkownika, czy też programy do wykrywania oprogramowania typu rootkit oraz dyski ratunkowe, których podstawowa funkcjonalność to wyszukiwanie, usuwanie lub poddawanie kwarantannie złośliwego oprogramowania.
5. Produkty z elementami cyfrowymi z funkcją wirtualnej sieci prywatnej (VPN)	Produkty z elementami cyfrowymi, które zestawiają zaszyfrowany tunel logiczny tworzony z wykorzystaniem zasobów systemowych sieci fizycznej lub wirtualnej. Kategoria ta obejmuje m.in. klienty wirtualnych sieci prywatnych, serwery wirtualnych sieci prywatnych i bramy wirtualnych sieci prywatnych.
6. Systemy zarządzania siecią	Produkty z elementami cyfrowymi, które zarządzają połączonymi elementami sieci, takimi jak serwery, routery, przełączniki, stacje robocze, drukarki lub urządzenia mobilne, poprzez ich monitorowanie oraz kontrolowanie ich konfiguracji i funkcjonowania w sieci. Kategoria ta obejmuje m.in. kompleksowe systemy zarządzania i specjalne systemy zarządzania konfiguracją, takie jak sterowniki programowalnych sieci komputerowych.
7. Systemy zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM)	Produkty z elementami cyfrowymi, które gromadzą dane z wielu źródeł, analizują i korelują te dane oraz prezentują je jako użyteczne informacje do celów związanych z bezpieczeństwem, takich jak wykrywanie zagrożeń i incydentów, analiza kryminalistyczna lub zgodność z przepisami.
8. Menedżery uruchamiania systemu	Oprogramowanie z elementami cyfrowymi, które zarządza procesem początkowego rozruchu systemu po włączeniu / ponownym uruchomieniu przez zainicjowanie pracy sprzętu, wczytanie środowiska systemu operacyjnego lub zasobów systemowych lub przekazanie kontroli systemowi operacyjnemu lub zasobom systemowym oraz przez wybór opcji rozruchu. Kategoria ta obejmuje m.in. oprogramowanie układowe UEFI, jednoetapowe i wieloetapowe programy rozruchowe.
9. Infrastruktura klucza publicznego i oprogramowanie do wystawiania certyfikatów cyfrowych	Produkty z elementami cyfrowymi wykorzystywane w ramach infrastruktury klucza publicznego (PKI), które zarządzają walidacją, tworzeniem, wydawaniem, dystrybucją, publikacją statusu, odnawianiem lub unieważnianiem certyfikatów cyfrowych lub generowaniem, przechowywaniem, deponowaniem, wymianą, niszczeniem lub rotacją kluczy kryptograficznych związanych z takimi certyfikatami cyfrowymi. Kategoria ta obejmuje m.in. systemy zarządzania kluczami, systemy zarządzania certyfikatami cyfrowymi, respondery OCSP (ang. online certificate status protocol) oraz kompleksowe rozwiązania PKI.

Kategoria produktów	Opis techniczny
10. Fizyczne i wirtualne interfejsy sieciowe	Fizyczne interfejsy sieciowe to produkty z elementami cyfrowymi, które odpowiadają za bezpośrednie połączenie urządzenia z siecią za pośrednictwem interfejsu programowania aplikacji (API) zapewnianego przez sterowniki interfejsu, zwykle działające w warstwie łącza danych, posiadające adaptery sprzętowe stanowiące interfejs z nośnikami transmisyjnymi wraz z odpowiednim oprogramowaniem układowym, zwykle działające w warstwie fizycznej i warstwie łącza danych. Wirtualne interfejsy sieciowe to produkty z elementami cyfrowymi, które odpowiadają za bezpośrednie lub pośrednie połączenie urządzenia z siecią za pośrednictwem API, który emuluje API sterowników fizycznych interfejsów sieciowych, zwykle działające w warstwie łącza danych. Kategoria ta obejmuje m.in. przewodowe i bezprzewodowe karty sieciowe, sterowniki i adaptery, takie jak Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee lub Fieldbus, a także samodzielne produkty mające wyłącznie postać wirtualną, takie jak wirtualne karty sieciowe, interfejsy CNI (Container Network Interface) i interfejsy VPN.
11. Systemy operacyjne	Oprogramowanie z elementami cyfrowymi, które zapewnia abstrakcyjny interfejs sprzętu, na którym jest zainstalowane, i steruje uruchamianiem oprogramowania oraz może świadczyć usługi takie jak zarządzanie zasobami obliczeniowymi i ich konfiguracja, planowanie, kontrola wejścia-wyjścia, zarządzanie danymi oraz zapewnianie interfejsu, za pośrednictwem którego aplikacje wchodzą w interakcję z zasobami systemowymi i urządzeniami peryferyjnymi. Kategoria ta obejmuje m.in. systemy operacyjne czasu rzeczywistego, systemy operacyjne ogólnego przeznaczenia i systemy operacyjne specjalnego przeznaczenia.
12. Routery, modemy przeznaczone do podłączenia do internetu oraz przełączniki	Routery to produkty z elementami cyfrowymi, które ustanawiają i kontrolują przepływ danych między różnymi sieciami poprzez wybór ścieżek lub tras z wykorzystaniem mechanizmów i algorytmów routingu, zwykle działające w warstwie sieciowej. Kategoria ta obejmuje m.in. routery przewodowe i bezprzewodowe, wirtualne routery i routery wyposażone w modem lub niezawierające modemu.
	Modemy przeznaczone do podłączenia do internetu (nawiązywania łączności z internetem) to produkty sprzętowe z elementami cyfrowymi, które wykorzystują techniki cyfrowej modulacji i demodulacji do przetwarzania sygnałów analogowych z i do sygnałów cyfrowych na potrzeby łączności opartej na protokole IP. Kategoria ta obejmuje m.in. modemy światłowodowe, modemy cyfrowej linii abonenckiej (DSL), modemy kablowe (DOCSIS), modemy satelitarne i modemy sieci komórkowej.
	Przełączniki to produkty z elementami cyfrowymi, które zapewniają łączność między urządzeniami sieciowymi za pomocą mechanizmów przesyłania pakietów danych i które mają płaszczyznę zarządzania, zazwyczaj wdrażane w warstwie łącza danych lub w warstwie sieciowej. Kategoria ta obejmuje m.in. zarządzane przełączniki, inteligentne przełączniki, przełączniki wielowarstwowe, wirtualne przełączniki z funkcjami bezpieczeństwa, programowalne przełączniki do programowalnej sieci komputerowej oraz mosty, takie jak punkty dostępu bezprzewodowego.

Kategoria produktów	Opis techniczny
13. Mikroprocesory z funkcjami bezpieczeństwa	Produkty z elementami cyfrowymi będące układami scalonymi, które wykonują funkcje centralnego przetwarzania z wykorzystaniem pamięci zewnętrznej i urządzeń peryferyjnych, obejmujące mikrokod i inne oprogramowanie układowe niskiego poziomu. Zapewniają dodatkowo funkcje związane z bezpieczeństwem, takie jak szyfrowanie, uwierzytelnianie, bezpieczne przechowywanie kluczy, generowanie liczb losowych, zaufane środowisko wykonawcze lub inne mechanizmy ochrony sprzętowej, których celem jest zabezpieczenie innych produktów, sieci lub usług wykraczających poza sam mikroprocesor, takich jak bezpieczny łańcuch rozruchu, wirtualizacja lub bezpieczne interfejsy komunikacyjne.
14. Mikrokontrolery z funkcjami bezpieczeństwa	Produkty z elementami cyfrowymi będące układami scalonymi, które wykonują funkcje centralnego przetwarzania, zawierające pamięć umożliwiającą programowanie mikrokontrolera, a także zazwyczaj również inne urządzenia peryferyjne, obejmujące mikrokod i inne oprogramowanie układowe niskiego poziomu. Zapewniają dodatkowo funkcje związane z bezpieczeństwem, takie jak szyfrowanie, uwierzytelnianie, bezpieczne przechowywanie kluczy, generowanie liczb losowych, zaufane środowisko wykonawcze lub inne mechanizmy ochrony sprzętowej, których celem jest zabezpieczenie innych produktów, sieci lub usług wykraczających poza sam mikrokontroler, takich jak bezpieczny łańcuch rozruchu, wirtualizacja lub bezpieczne interfejsy komunikacyjne.
15. Specjalizowane układy scalone (ASIC) i bezpośrednio programowalne macierze bramek (FPGA) z funkcjami bezpieczeństwa	Specjalizowane układy scalone (ASIC) z funkcjami bezpieczeństwa to produkty z elementami cyfrowymi będące układami scalonymi, zaprojektowane całkowicie lub częściowo na indywidualne zamówienie w celu pełnienia określonej funkcji lub wdrożenia określonej aplikacji, obejmujące mikrokod i inne oprogramowanie układowe niskiego poziomu. Zapewniają dodatkowo funkcje związane z bezpieczeństwem, takie jak szyfrowanie, uwierzytelnianie, bezpieczne przechowywanie kluczy, generowanie liczb losowych, zaufane środowisko wykonawcze lub inne mechanizmy ochrony sprzętowej, które mają na celu zabezpieczenie innych produktów, sieci lub usług wykraczających poza same ASIC, takich jak bezpieczny łańcuch rozruchu, wirtualizacja lub bezpieczne interfejsy komunikacyjne.
	Programowalne macierze bramek (FPGA) z funkcjami bezpieczeństwa to produkty z elementami cyfrowymi, które są układami scalonymi charakteryzującymi się macierzą konfigurowalnych bloków logicznych zaprojektowanych tak, aby można je było przeprogramować po wytworzeniu, by mogły pełnić określoną funkcję lub wdrożyć określoną aplikację, obejmujące mikrokod i inne oprogramowanie układowe niskiego poziomu. Zapewniają dodatkowo funkcje związane z bezpieczeństwem, takie jak szyfrowanie, uwierzytelnianie, bezpieczne przechowywanie kluczy, generowanie liczb losowych, zaufane środowisko wykonawcze lub inne mechanizmy ochrony sprzętowej, które mają na celu zabezpieczenie innych produktów, sieci lub usług wykraczających poza same FPGA, takich jak bezpieczny łańcuch rozruchu, wirtualizacja lub bezpieczne interfejsy komunikacyjne.
16. Wirtualni asystenci inteligentnego domu ogólnego przeznaczenia	Produkty z elementami cyfrowymi komunikujące się w oparciu o publiczny internet bezpośrednio lub za pośrednictwem innego sprzętu, które przetwarzają żądania, zadania lub pytania formułowane w oparciu o język naturalny, na przykład zapytania w formie dźwiękowej lub pisemnej, oraz które na podstawie tych żądań, zadań lub pytań zapewniają dostęp do innych usług lub kontrolują funkcje urządzeń podłączonych do internetu w środowisku domowym. Kategoria ta obejmuje m.in. inteligentne głośniki ze zintegrowanym wirtualnym asystentem oraz samodzielnych wirtualnych asystentów, którzy odpowiadają temu opisowi.

Kategoria produktów	Opis techniczny
17. Produkty inteligentnego domu z funkcjami bezpieczeństwa, w tym inteligentne zamki do drzwi, kamery systemów bezpieczeństwa, nianie elektroniczne i systemy alarmowe	Produkty z elementami cyfrowymi, które chronią bezpieczeństwo fizyczne konsumentów w środowisku domowym i którymi można sterować lub zarządzać zdalnie za pomocą innych systemów, a także sprzęt i oprogramowanie, które centralnie sterują takimi produktami. Kategoria ta obejmuje m.in. inteligentne urządzenia do zamykania drzwi, nianie elektroniczne, systemy alarmowe i domowe kamery systemów bezpieczeństwa.
18. Zabawki podłączone do internetu objęte dyrektywą Parlamentu Europejskiego i Rady 2009/48/WE ([1]) z interaktywnymi funkcjami społecznymi (np. mówienie lub filmowanie) lub z funkcją śledzenia lokalizacji	Zabawki podłączone do internetu z interaktywnymi funkcjami społecznymi to produkty z elementami cyfrowymi objęte dyrektywą 2009/48/WE, komunikujące się w oparciu o publiczny internet bezpośrednio lub za pośrednictwem jakiegokolwiek innego sprzętu, w które wbudowano rozwiązania technologiczne umożliwiające komunikację przychodzącą i wychodzącą, takie jak klawiatura, mikrofon, głośnik lub kamera.
	Zabawki podłączone do internetu z funkcją śledzenia lokalizacji to produkty z elementami cyfrowymi objęte dyrektywą 2009/48/WE, komunikujące się w oparciu o publiczny internet bezpośrednio lub za pośrednictwem jakiegokolwiek innego sprzętu, które wyposażono w technologie umożliwiające śledzenie lub ustalenie położenia geograficznego zabawki lub jej użytkownika. Jeżeli dana zabawka wykrywa jedynie bliskość użytkownika lub innych zabawek za pomocą technologii czujnikowych, zabawki tej nie uznaje się za mającą funkcje śledzenia lokalizacji.
19. Produkty do noszenia lub umieszczania na ciele ludzkim mające monitorować stan zdrowia (np. śledzące aktywność fizyczną), do których nie stosuje się rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 ([2]) ani rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746 ([3]), lub przedmioty osobiste do noszenia na ciele, które mają być używane przez dzieci i dla dzieci	Produkty do noszenia lub umieszczania na ciele ludzkim mające monitorować stan zdrowia to produkty z elementami cyfrowymi, które są noszone na ciele bezpośrednio lub za pośrednictwem odzieży lub dodatków i które mogą, regularnie lub w sposób ciągły, odczytywać i dalej przetwarzać informacje, w tym parametry fizjologiczne, istotne dla zdrowia użytkownika, z wyłączeniem produktów objętych zakresem rozporządzenia (UE) 2017/745 lub rozporządzenia (UE) 2017/746. Kategoria ta obejmuje m.in. urządzenia do monitorowania aktywności fizycznej, inteligentne zegarki, inteligentną biżuterię, inteligentną odzież i odzież sportową, które odpowiadają temu opisowi.
	Przedmioty osobiste do noszenia na ciele, które mają być używane przez dzieci i dla dzieci, to produkty z elementami cyfrowymi, które mogą być noszone lub umieszczane na ciele, bezpośrednio lub za pomocą odzieży lub dodatków, u osób w wieku poniżej 14 lat. Kategoria ta obejmuje m.in. produkty zabezpieczające dla dzieci przeznaczone do noszenia na ciele.

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2009/48/WE z dnia 18 czerwca 2009 r. w sprawie bezpieczeństwa zabawek (Dz.U. L 170 z 30.6.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.U. L 117 z 5.5.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz.U. L 117 z 5.5.2017, s. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Klasa II

Kategoria produktów	Opis techniczny
1. Hiperwizory i systemy środowiska uruchomieniowego, które wspomagają zwirtualizowane uruchamianie systemów operacyjnych i podobnych środowisk	Hiperwizory to oprogramowanie z elementami cyfrowymi, które dokonuje wirtualizacji zasobów obliczeniowych lub je przydziela i umożliwia uruchamianie i organizację maszyn wirtualnych, które są logicznie oddzielone od siebie lub od sprzętu fizycznego, oraz zarządzanie nimi. Hiperwizory mogą działać bezpośrednio na poziomie sprzętu (hiperwizory natywne, ang. bare metal), w systemie operacyjnym lub w innej wirtualnej maszynie (zagnieżdżona wirtualizacja). W kontekście tej kategorii produktów maszyna wirtualna to logicznie odizolowane, definiowane programowo środowisko obliczeniowe, które obejmuje wirtualny zestaw zasobów sprzętowych (np. procesor, pamięć operacyjna, pamięć masowa, interfejsy sieciowe) i zazwyczaj obsługuje własny system operacyjny. Kategoria ta obejmuje m.in. hiperwizory typu 1 (natywne, ang. bare metal), hiperwizory typu 2 (uruchamiane w systemie operacyjnym) i hiperwizory hybrydowe.
	Systemy środowiska uruchomieniowego to oprogramowanie z elementami cyfrowymi, które zarządza uruchamianiem i cyklem życia kontenerów eksploatowanych w systemie operacyjnym pojedynczego hosta jako odizolowane procesy, przydzielając zasoby i umożliwiając zarządzanie pojedynczymi kontenerami i ich organizację. W kontekście tej kategorii produktów kontener to środowisko wykonawcze oparte na oprogramowaniu, które obejmuje co najmniej jeden komponent oprogramowania i jego zależności w jednym pakiecie, co umożliwia niezależne i spójne działanie.
2. Zapory sieciowe, systemy wykrywania włamań lub zapobiegania włamaniom	Zapory sieciowe to produkty z elementami cyfrowymi, które chronią połączoną sieć lub połączony system przed nieuprawnionym dostępem poprzez monitorowanie i ograniczanie przesyłu danych do i z tej sieci. Kategoria ta obejmuje m.in. zapory sieciowe i zapory aplikacji, takie jak zapory aplikacji internetowych bądź filtry oraz bramki antyspamowe.
	Systemy wykrywania włamań to produkty z elementami cyfrowymi, które monitorują ruch trafiający do środowiska sieciowego pod kątem podejrzanej działalności i wykrywają lub wskazują, czy podjęto próbę włamania do połączonej sieci lub połączonego systemu lub czy takie włamanie ma lub miało miejsce. Kategoria ta obejmuje m.in. systemy wykrywania włamań działające na poziomie sieci i systemy wykrywania włamań działające na poziomie hosta.
	Systemy zapobiegania włamaniom to produkty z elementami cyfrowymi składające się z systemu wykrywania włamań, który aktywnie reaguje na włamanie do połączonej sieci lub połączonego systemu. Kategoria ta obejmuje m.in. systemy zapobiegania włamaniom działające na poziomie sieci i systemy zapobiegania włamaniom działające na poziomie hosta.

Kategoria produktów	Opis techniczny
3. Mikroprocesory odporne na manipulacje	Produkty z elementami cyfrowymi, które są mikroprocesorami z funkcjami bezpieczeństwa, o których mowa w tabeli „Klasa I" pkt 13 niniejszego załącznika, obejmującymi mechanizmy umożliwiające stwierdzenie manipulacji, zapewnienie odporności na manipulacje lub reagowanie na manipulacje, i które dodatkowo zostały zaprojektowane w celu zapewnienia ochrony na poziomie AVA_VAN 2 lub 3, jak określono we wspólnych kryteriach i wspólnej metodyce oceny.
4. Mikrokontrolery odporne na manipulacje	Produkty z elementami cyfrowymi, które są mikrokontrolerami z funkcjami bezpieczeństwa, o których mowa w tabeli „Klasa I" pkt 14 niniejszego załącznika, zawierające mechanizmy umożliwiające stwierdzenie manipulacji, zapewnienie odporności na manipulacje lub reagowanie na manipulacje, i które dodatkowo zostały zaprojektowane tak, aby zapewnić ochronę na poziomie AVA_VAN 2 lub 3, jak określono we wspólnych kryteriach i wspólnej metodyce oceny.

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

ZAŁĄCZNIK II

PRODUKTY KRYTYCZNE Z ELEMENTAMI CYFROWYMI

Kategoria produktów	Opis techniczny
1. Urządzenia sprzętowe ze skrzynkami zabezpieczającymi	Urządzenia sprzętowe z elementami cyfrowymi, które w bezpieczny sposób przechowują i przetwarzają dane wrażliwe, zarządzają nimi lub wykonują operacje kryptograficzne i które składają się z wielu oddzielnych komponentów, zawierające fizyczną obudowę sprzętu zapewniającą możliwość stwierdzenia manipulacji, zapewniającą odporność na manipulacje lub umożliwiającą reagowanie na manipulacje jako środki przeciwdziałania atakom fizycznym. Kategoria ta obejmuje m.in. fizyczne terminale płatnicze, sprzętowe moduły bezpieczeństwa, które generują elementy kryptograficzne i nimi zarządzają, oraz tachografy, które odpowiadają powyższemu opisowi.
2. Bramy inteligentnych liczników w inteligentnych systemach pomiarowych zdefiniowanych w art. 2 pkt 23 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/944 [1] oraz inne urządzenia do zaawansowanych celów bezpieczeństwa, w tym do bezpiecznego kryptoprzetwarzania	Bramy inteligentnych liczników to produkty z elementami cyfrowymi, które sterują komunikacją między komponentami w inteligentnych systemach opomiarowania zdefiniowanych w art. 2 pkt 23 dyrektywy (UE) 2019/944 lub podłączonymi do nich a upoważnionymi osobami trzecimi, takimi jak dostawcy usług użyteczności publicznej. Bramy inteligentnych liczników gromadzą, przetwarzają i przechowują dane pomiarowe lub dane osobowe, chronią przepływ danych i informacji poprzez wspieranie szczególnych potrzeb kryptograficznych, takich jak szyfrowanie i odszyfrowywanie danych, posiadają funkcje zapory i zapewniają środki do sterowania innymi urządzeniami. Kategoria ta obejmuje m.in. bramy inteligentnych liczników związane z inteligentnymi systemami opomiarowania służącymi do pomiaru energii elektrycznej zdefiniowanymi w art. 2 pkt 23 dyrektywy (UE) 2019/944. Może ona również obejmować bramy inteligentnych liczników wykorzystywane w innych inteligentnych systemach pomiarowych mierzących zużycie innych źródeł energii, takich jak gaz lub ciepło, pod warunkiem że brama odpowiada temu opisowi.
3. Karty inteligentne lub podobne urządzenia, w tym elementy zabezpieczające	Elementy zabezpieczające to mikrokontrolery lub mikroprocesory z funkcjami bezpieczeństwa, które obejmują mechanizmy umożliwiające stwierdzenie manipulacji, zapewnienie odporności na manipulacje lub reagowanie na manipulacje. Zazwyczaj przechowują lub przetwarzają operacje kryptograficzne lub dane wrażliwe, takie jak poświadczenia tożsamości lub dane uwierzytelniające płatności, lub zarządzają nimi. Elementy zabezpieczające są zaprojektowane w taki sposób, aby zapewnić ochronę co najmniej na poziomie AVA_VAN.4, jak określono we wspólnych kryteriach lub we wspólnej metodyce oceny. Mogą to być odrębne komponenty krzemowe lub mogą one być zintegrowane w układzie SoC (ang. System on a Chip). Elementy zabezpieczające mogą mieć wbudowane środowisko aplikacji lub system operacyjny i mogą zawierać aplikację lub aplikacje. Kategoria ta obejmuje m.in. moduły zaufanej platformy (TPM) i wbudowane uniwersalne karty z układem scalonym (UICC).
	Karty elektroniczne lub podobne urządzenia są elementami zabezpieczającymi zintegrowanymi z materiałem nośnikowym w kształcie karty, takim jak tworzywo sztuczne lub drewno, lub elementami zabezpieczającymi zintegrowanymi z materiałami nośnikowymi o innych kształtach. Kategoria ta obejmuje m.in. dokumenty tożsamości i dokumenty podróży, karty z certyfikatem podpisu kwalifikowanego, wymienne uniwersalne karty z układem scalonym, fizyczne karty płatnicze, fizyczne karty dostępu, karty do tachografów cyfrowych lub opaski ze zintegrowanymi elementami zabezpieczającymi płatności.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej oraz zmieniająca dyrektywę 2012/27/UE (Dz.U. L 158 z 14.6.2019, s. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).