# 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)

**(Tekst mający znaczenie dla EOG)**

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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) ([1]), w szczególności jego art. 49 ust. 7,

a także mając na uwadze, co następuje:

(1) W niniejszym rozporządzeniu określono role, zasady i obowiązki, a także strukturę europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) zgodnie z europejskimi ramami certyfikacji cyberbezpieczeństwa określonymi w rozporządzeniu (UE) 2019/881. EUCC opiera się na umowie o wzajemnym uznawaniu certyfikatów bezpieczeństwa technologii informacyjnych zatwierdzonej przez Grupę Wyższych Urzędników ds. Bezpieczeństwa Systemów Informatycznych ([2]) („SOG-IS") z wykorzystaniem wspólnych kryteriów, w tym procedur i dokumentów grupy.

(2) Program powinien opierać się na ustalonych normach międzynarodowych. Wspólne kryteria to międzynarodowa norma dotycząca oceny bezpieczeństwa informacji, opublikowana na przykład jako ISO/IEC 15408 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kryteria oceny zabezpieczeń informatycznych. Opiera się ona na ocenie dokonanej przez osobę trzecią i obejmuje siedem poziomów uzasadnienia zaufania („EAL"). Wspólnym kryteriom towarzyszy wspólna metodyka oceny, opublikowana na przykład jako ISO/IEC 18045 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kryteria oceny zabezpieczeń informatycznych – Metodyka oceny zabezpieczeń informatycznych. Specyfikacje i dokumenty, w których stosuje się przepisy niniejszego rozporządzenia, mogą odnosić się do publicznie dostępnej normy, która odzwierciedla normę stosowaną w certyfikacji na podstawie niniejszego rozporządzenia, taką jak wspólne kryteria oceny bezpieczeństwa technologii informacyjnych i wspólna metodyka oceny bezpieczeństwa technologii informacyjnych.

(3) EUCC wykorzystuje rodzinę oceny podatności (AVA_VAN) według wspólnych kryteriów, komponenty 1–5. Te pięć komponentów zapewnia wszystkie główne wyznaczniki i zależności do analizy podatności produktów ICT. Ponieważ komponenty odpowiadają poziomom uzasadnienia zaufania określonym w niniejszym rozporządzeniu, pozwalają one na świadomy wybór uzasadnienia zaufania na podstawie przeprowadzonych ocen wymogów bezpieczeństwa i ryzyka związanego z przewidzianym stosowaniem produktu ICT. Wnioskodawca ubiegający się o certyfikat EUCC powinien przedstawić dokumentację związaną z przewidzianym stosowaniem produktu ICT oraz analizę poziomów ryzyka związanego z takim stosowaniem, aby umożliwić jednostce oceniającej zgodność ocenę odpowiedniości wybranego poziomu uzasadnienia zaufania. W przypadku gdy działania w zakresie oceny i certyfikacji wykonuje ta sama jednostka oceniająca zgodność, wnioskodawca powinien przedłożyć wymagane informacje tylko raz.

(4) Domena techniczna to ramy odniesienia obejmujące grupę produktów ICT, które mają określone i podobne funkcje bezpieczeństwa ograniczające ataki, których cechy są wspólne dla danego poziomu uzasadnienia zaufania. Domena techniczna opisuje w dokumentach odzwierciedlających stan wiedzy określone wymagania bezpieczeństwa, a także dodatkowe metody, techniki i narzędzia oceny, które mają zastosowanie do certyfikacji produktów ICT objętych tą domeną techniczną. Domena techniczna sprzyja zatem również harmonizacji oceny objętych nią produktów ICT. W przypadku certyfikacji na poziomach AVA_VAN.4 i AVA_VAN.5 obecnie stosuje się powszechnie dwie domeny

([1]) Dz.U. L 151 z 7.6.2019, s. 15.

([2]) Umowa o wzajemnym uznawaniu certyfikatów oceny bezpieczeństwa technologii informacyjnych, wersja 3.0 ze stycznia 2010 r., dostępna na stronie sogis.eu, zatwierdzona przez Grupę Wyższych Urzędników Komisji Europejskiej ds. Bezpieczeństwa Systemów Informatycznych w odpowiedzi na pkt 3 zalecenia Rady 95/144/WE z dnia 7 kwietnia 1995 r. w sprawie wspólnych kryteriów oceny bezpieczeństwa technologii informacyjnych (Dz.U. L 93 z 26.4.1995, s. 27).

techniczne. Pierwszą domeną techniczną jest domena techniczna „Karty elektroniczne i podobne urządzenia", w której znaczna część wymaganych funkcji bezpieczeństwa zależy od konkretnych, dostosowanych do potrzeb elementów sprzętu, które często można rozdzielić (np. sprzęt do kart elektronicznych, układy scalone, produkty złożone kart elektronicznych, moduły zaufanej platformy stosowane w ramach zaufanego przetwarzania danych lub karty do tachografów cyfrowych). Drugą domeną techniczną jest domena „Urządzenie sprzętowe ze skrzynkami bezpieczeństwa", w której znaczna część wymaganych funkcji bezpieczeństwa zależy od fizycznej obudowy sprzętu (zwanej „skrzynką bezpieczeństwa") zaprojektowanej tak, aby była odporna na bezpośrednie ataki, np. terminale płatnicze, przyrządy rejestrujące tachografów, inteligentne liczniki, terminale kontroli dostępu i sprzętowe moduły bezpieczeństwa.

(5) Składając wniosek o certyfikację, wnioskodawca powinien odnieść swoje uzasadnienie wyboru poziomu uzasadnienia zaufania do celów określonych w art. 51 rozporządzenia (UE) 2019/881 oraz do wyboru komponentów z katalogu funkcjonalnych wymogów bezpieczeństwa i wymogów uzasadnienia zaufania do bezpieczeństwa zawartych we wspólnych kryteriach. Jednostka certyfikująca powinna ocenić adekwatność wybranego poziomu uzasadnienia zaufania i zapewnić, aby wybrany poziom był proporcjonalny do poziomu ryzyka związanego z przewidzianym stosowaniem produktu ICT.

(6) Zgodnie ze wspólnymi kryteriami certyfikację przeprowadza się w odniesieniu do celu bezpieczeństwa, który obejmuje określenie problemu w zakresie bezpieczeństwa produktu ICT, a także celów bezpieczeństwa, które przeciwdziałają problemowi w zakresie bezpieczeństwa. Problem w zakresie bezpieczeństwa dostarcza szczegółowych informacji na temat przewidzianego stosowania produktu ICT i zagrożeń związanych z takim stosowaniem. Wybrany zestaw wymogów bezpieczeństwa odpowiada zarówno problemowi w zakresie bezpieczeństwa, jak i celom bezpieczeństwa produktu ICT.

(7) Profile zabezpieczeń są skutecznym sposobem wstępnego określenia wspólnych kryteriów, które mają zastosowanie do danej kategorii produktów ICT, a zatem są również istotnym elementem procesu certyfikacji produktów ICT objętych profilem zabezpieczeń. Profil zabezpieczeń wykorzystuje się do oceny przyszłych celów bezpieczeństwa, które wchodzą w zakres danej kategorii produktów ICT objętych tym profilem zabezpieczeń. Usprawniają one i zwiększają efektywność procesu certyfikacji produktów ICT oraz pomagają użytkownikom w prawidłowym i skutecznym określeniu funkcjonalności produktu ICT. Profile zabezpieczeń należy zatem uważać za integralną część procesu ICT prowadzącego do certyfikacji produktów ICT.

(8) Aby profile zabezpieczeń mogły pełnić swoją rolę w procesie ICT wspierającym rozwijanie i dostarczanie certyfikowanego produktu ICT, powinna istnieć możliwość ich certyfikacji niezależnie od certyfikacji określonego produktu ICT objętego odpowiednim profilem zabezpieczeń. W celu zapewnienia wysokiego poziomu cyberbezpieczeństwa konieczne jest zatem stosowanie co najmniej takiego samego poziomu kontroli do profili zabezpieczeń i do celów bezpieczeństwa. Profile zabezpieczeń należy oceniać i certyfikować oddzielnie od powiązanego produktu ICT i wyłącznie poprzez zastosowanie klasy uzasadnienia zaufania określonej we wspólnych kryteriach i wspólnej metodyce oceny w odniesieniu do profili zabezpieczeń (APE) oraz, w stosownych przypadkach, konfiguracji profili zabezpieczeń (ACE). Ze względu na ich ważną i delikatną rolę jako punktu odniesienia w certyfikacji produktów ICT powinny one być certyfikowane wyłącznie przez organy publiczne lub przez jednostkę certyfikującą, która uzyskała uprzednią zgodę krajowego organu ds. certyfikacji cyberbezpieczeństwa w odniesieniu do danego profilu zabezpieczeń. Ze względu na ich zasadniczą rolę w certyfikacji na poziomie uzasadnienia zaufania „wysoki", w szczególności poza domenami technicznymi, profile zabezpieczeń należy opracowywać jako dokumenty odzwierciedlające stan wiedzy, które powinny zostać zatwierdzone przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa.

(9) Certyfikowane profile zabezpieczeń należy uwzględniać przy monitorowaniu zgodności z EUCC i jego przestrzegania przez krajowe organy ds. certyfikacji cyberbezpieczeństwa. W przypadku gdy metodyka, narzędzia i umiejętności stosowane w podejściach do oceny produktów ICT są dostępne w odniesieniu do konkretnych certyfikowanych profili zabezpieczeń, domeny techniczne mogą opierać się na tych konkretnych profilach zabezpieczeń.

(10) Aby osiągnąć wysoki poziom zaufania i uzasadnienia zaufania w odniesieniu do certyfikowanych produktów ICT, na podstawie niniejszego rozporządzenia nie należy zezwalać na ocenę przez stronę pierwszą. Powinna być dozwolona wyłącznie ocena zgodności przez stronę trzecią dokonywana przez ITSEF i jednostki certyfikujące.

(11) Społeczność SOG-IS zapewniła wspólne interpretacje i podejścia w zakresie stosowania wspólnych kryteriów i wspólną metodykę oceny w certyfikacji, w szczególności w odniesieniu do poziomu uzasadnienia zaufania „wysoki" zapewnianego przez domeny techniczne „Karty elektroniczne i podobne urządzenia" oraz „Urządzenie sprzętowe ze skrzynkami bezpieczeństwa". Ponowne wykorzystanie takich dokumentów pomocniczych w programie EUCC zapewnia płynne przejście od wdrożonych na szczeblu krajowym programów SOG-IS do zharmonizowanego programu EUCC. W związku z tym w niniejszym rozporządzeniu należy uwzględnić zharmonizowane metodyki oceny o ogólnym znaczeniu dla wszystkich działań w zakresie certyfikacji. Ponadto Komisja powinna mieć możliwość zwrócenia się do Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa o przyjęcie opinii zatwierdzającej i zalecającej stosowanie metodyk oceny określonych w dokumentach odzwierciedlających stan wiedzy dotyczących certyfikacji produktu ICT lub profilu zabezpieczeń w ramach programu EUCC. W załączniku I do niniejszego rozporządzenia wymieniono zatem dokumenty odzwierciedlające stan wiedzy dotyczące działań w zakresie oceny prowadzonych przez jednostki oceniające zgodność. Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa powinna zatwierdzać i utrzymywać dokumenty odzwierciedlające stan wiedzy. Dokumenty odzwierciedlające stan wiedzy należy wykorzystywać przy certyfikacji. Jednostka oceniająca zgodność może ich nie wykorzystać wyłącznie w wyjątkowych i należycie uzasadnionych przypadkach, z zastrzeżeniem spełnienia określonych warunków, w szczególności zatwierdzenia przez krajowy organ ds. certyfikacji cyberbezpieczeństwa.

(12) Certyfikacja produktów ICT na poziomie AVA_VAN 4 lub 5 powinna być możliwa wyłącznie na określonych warunkach i w przypadku gdy dostępna jest szczegółowa metodyka oceny. Szczegółowa metodyka oceny może być zapisana w dokumentach odzwierciedlających stan wiedzy właściwych dla danej domeny technicznej lub w szczególnych profilach zabezpieczeń przyjętych jako dokument odzwierciedlający stan wiedzy właściwych dla danej kategorii produktu. Certyfikacja na tych poziomach uzasadnienia zaufania powinna być możliwa wyłącznie w wyjątkowych i należycie uzasadnionych przypadkach, z zastrzeżeniem szczególnych warunków, w szczególności zatwierdzenia przez krajowy organ ds. certyfikacji cyberbezpieczeństwa, w tym w odniesieniu do mającej zastosowanie metodyki oceny. Takie wyjątkowe i należycie uzasadnione przypadki mogą wystąpić, gdy przepisy unijne lub krajowe wymagają certyfikacji produktu ICT na poziomie AVA_VAN 4 lub 5. Podobnie w wyjątkowych i należycie uzasadnionych przypadkach profile zabezpieczeń mogą być certyfikowane bez zastosowania odpowiednich dokumentów odzwierciedlających stan wiedzy, z zastrzeżeniem szczególnych warunków, w szczególności zatwierdzenia przez krajowy organ ds. certyfikacji cyberbezpieczeństwa, w tym w odniesieniu do mającej zastosowanie metodyki oceny.

(13) Znaki i etykiety stosowane w ramach EUCC mają na celu wykazanie użytkownikom wiarygodności certyfikowanego produktu ICT i umożliwienie im dokonania świadomego wyboru przy zakupie produktów ICT. Stosowanie znaków i etykiet powinno również podlegać regułom i warunkom określonym w normie ISO/IEC 17065 oraz, w stosownych przypadkach, normie ISO/IEC 17030 wraz z odpowiednimi wytycznymi.

(14) Jednostki certyfikujące powinny decydować o okresie ważności certyfikatów, biorąc pod uwagę cykl życia danego produktu ICT. Okres ważności nie powinien przekraczać 5 lat. Krajowe organy ds. certyfikacji cyberbezpieczeństwa powinny pracować nad ujednoliceniem okresu ważności w Unii.

(15) W przypadku zmniejszenia zakresu istniejącego certyfikatu EUCC certyfikat ten zostaje wycofany i należy wydać nowy certyfikat mający nowy zakres, aby zapewnić jasne informowanie użytkowników o obecnym zakresie i poziomie uzasadnienia zaufania certyfikatu danego produktu ICT.

(16) Certyfikacja profili zabezpieczeń różni się od certyfikacji produktów ICT, ponieważ dotyczy procesu ICT. Ponieważ profil zabezpieczeń obejmuje kategorię produktów ICT, jego oceny i certyfikacji nie można przeprowadzić na podstawie pojedynczego produktu ICT. Ponieważ profil zabezpieczeń ujednolica ogólne wymogi bezpieczeństwa dotyczące kategorii produktów ICT i jest niezależny od tego, w jaki sposób produkt ICT jest przedstawiany przez jego sprzedawcę, okres ważności certyfikatu EUCC dla profilu zabezpieczeń powinien zasadniczo wynosić co najmniej 5 lat i może zostać przedłużony na cały okres obowiązywania profilu zabezpieczeń.

(17) Jednostkę oceniającą zgodność definiuje się jako jednostkę, która wykonuje czynności z zakresu oceny zgodności, w tym wzorcowanie, badanie, certyfikację i inspekcję. Aby zapewnić wysoką jakość usług, w niniejszym rozporządzeniu określono, że działalność w zakresie wzorcowania, z jednej strony, oraz działalność w zakresie certyfikacji i inspekcji, z drugiej strony, powinna być prowadzona przez podmioty działające niezależnie od siebie, a mianowicie, odpowiednio, jednostki oceniające bezpieczeństwo technologii informacyjnych („ITSEF") i jednostki certyfikujące. Oba rodzaje jednostek oceniających zgodność powinny zostać akredytowane i, w stosownych przypadkach, należy udzielić im zezwolenia.

(18) Jednostka certyfikująca powinna być akredytowana zgodnie z normą ISO/IEC 17065 przez krajową jednostkę akredytującą dla poziomów uzasadnienia zaufania „istotny" i „wysoki". Oprócz akredytacji zgodnie z rozporządzeniem (UE) 2019/881 w związku z rozporządzeniem (WE) nr 765/2008 jednostki oceniające zgodność powinny spełniać określone wymogi, stanowiące gwarancję ich kwalifikacji technicznych do oceny wymogów cyberbezpieczeństwa w ramach poziomu uzasadnienia zaufania „wysoki" EUCC, co jest potwierdzane „zezwoleniem". Aby wesprzeć proces udzielania zezwoleń, odpowiednie dokumenty odzwierciedlające stan wiedzy powinny zostać opracowane i powinny zostać opublikowane przez ENISA po zatwierdzeniu przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa.

(19) Kwalifikacje techniczne ITSEF należy oceniać poprzez akredytację laboratorium badawczego zgodnie z normą ISO/IEC 17025 i uzupełnić normą ISO/IEC 23532-1 w odniesieniu do pełnego zestawu działań w zakresie oceny, które są istotne dla poziomu uzasadnienia zaufania i określone w normie ISO/IEC 18045 w związku z normą ISO/IEC 15408. Zarówno jednostka certyfikująca, jak i ITSEF powinny ustanowić i utrzymywać odpowiedni system zarządzania kompetencjami personelu, który to system opiera się na normie ISO/IEC 19896-1 w odniesieniu do elementów i poziomów kompetencji oraz oceny kompetencji. W odniesieniu do poziomu wiedzy, umiejętności, doświadczenia i wykształcenia, mające zastosowanie wymogi wobec osób oceniających powinny wynikać z normy ISO/IEC 19896-3. Należy wykazać równoważne przepisy i środki dotyczące odstępstw od takich systemów zarządzania kompetencjami, zgodnie z celami systemu.

(20) Aby uzyskać zezwolenie, ITSEF powinna wykazać swoją zdolność do określenia braku znanych podatności, prawidłowego i spójnego wdrożenia nowoczesnych funkcjonalności bezpieczeństwa dla danej technologii oraz odporności wskazanego produktu ICT na zaawansowane ataki. Ponadto w przypadku zezwoleń w domenie technicznej „Karty elektroniczne i podobne urządzenia" ITSEF powinna również wykazać zdolności techniczne niezbędne do działań w zakresie oceny i powiązanych zadań określonych w dokumencie uzupełniającym „Minimalne wymogi ITSEF dotyczące ocen bezpieczeństwa kart elektronicznych i podobnych urządzeń" ([3]) zgodnie ze wspólnymi kryteriami. W przypadku zezwolenia w domenie technicznej „Urządzenie sprzętowe ze skrzynkami bezpieczeństwa" ITSEF powinna ponadto wykazać minimalne wymogi techniczne niezbędne do przeprowadzania działań w zakresie oceny i powiązanych zadań dotyczących urządzeń sprzętowych ze skrzynkami bezpieczeństwa, zgodnie z zaleceniami ECCG. W kontekście minimalnych wymogów ITSEF musi mieć możliwość przeprowadzania poszczególnych rodzajów ataków określonych w dokumencie uzupełniającym „Zastosowanie potencjału ataku do urządzeń sprzętowych ze skrzynkami bezpieczeństwa" zgodnie ze wspólnymi kryteriami. Możliwości te obejmują wiedzę i umiejętności osoby oceniającej oraz sprzęt i metody oceny potrzebne do określenia i oceny poszczególnych rodzajów ataków.

(21) Krajowy organ ds. certyfikacji cyberbezpieczeństwa powinien monitorować wypełnianie przez jednostki certyfikujące, ITSEF i posiadaczy certyfikatów obowiązków wynikających z niniejszego rozporządzenia i rozporządzenia (UE) 2019/881. Krajowy organ ds. certyfikacji cyberbezpieczeństwa powinien wykorzystywać w tym celu wszelkie odpowiednie źródła informacji, w tym informacje otrzymane od uczestników procesu certyfikacji oraz własne dochodzenia.

(22) Jednostki certyfikujące powinny współpracować z odpowiednimi organami nadzoru rynku i uwzględniać wszelkie informacje o podatnościach, które mogą być istotne dla produktów ICT, dla których wydały certyfikaty. Jednostki certyfikujące powinny monitorować certyfikowane przez nie profile zabezpieczeń w celu ustalenia, czy wymogi bezpieczeństwa określone dla danej kategorii produktów ICT nadal odzwierciedlają najnowsze zmiany w krajobrazie zagrożeń.

(23) Aby wspierać monitorowanie zgodności, krajowe organy ds. certyfikacji cyberbezpieczeństwa powinny współpracować z odpowiednimi organami nadzoru rynku zgodnie z art. 58 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 ([4]). Podmioty gospodarcze w Unii mają obowiązek wymiany informacji i współpracy z organami nadzoru rynku zgodnie z art. 4 ust. 3 rozporządzenia 2019/1020.

([3]) Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices [Wspólna biblioteka interpretacji: Minimalne wymogi ITSEF dotyczące oceny bezpieczeństwa kart elektronicznych i podobnych urządzeń], wersja 2.1 z lutego 2020 r., dostępna pod adresem sogis.eu.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.U. L 169 z 25.6.2019, s. 1).

(24) Jednostki certyfikujące powinny monitorować przestrzeganie wymogów przez posiadaczy certyfikatów oraz zgodność wszystkich certyfikatów wydanych w ramach EUCC. Monitorowanie powinno zapewniać, aby wszystkie sprawozdania z oceny przedstawiane przez ITSEF oraz wnioski w nich zawarte, a także kryteria i metody oceny były stosowane w sposób jednolity i prawidłowy we wszystkich działaniach w zakresie certyfikacji.

(25) W przypadku wykrycia potencjalnych przypadków niezgodności, które mają wpływ na certyfikowany produkt ICT, ważne jest zapewnienie proporcjonalnej reakcji. Certyfikaty mogą zatem zostać zawieszone. Zawieszenie powinno wiązać się z określonymi ograniczeniami dotyczącymi promowania i użytkowania danego produktu ICT, ale nie powinno wpływać na ważność certyfikatu. O zawieszeniu nabywcy danych produktów ICT powinni zostać powiadomieni przez posiadacza certyfikatu UE, natomiast odpowiednie organy nadzoru rynku powinny zostać powiadomione przez właściwy krajowy organ ds. certyfikacji cyberbezpieczeństwa. Aby poinformować opinię publiczną, ENISA powinna opublikować informacje o zawieszeniu na specjalnej stronie internetowej.

(26) Posiadacz certyfikatu EUCC powinien wdrożyć niezbędne procedury zarządzania podatnościami i zapewnić, aby procedury te stanowiły integralną część jego organizacji. Po uzyskaniu informacji na temat potencjalnej podatności posiadacz certyfikatu EUCC powinien przeprowadzić analizę skutków podatności. W przypadku gdy analiza skutków podatności potwierdzi, że podatność może zostać wykorzystana, posiadacz certyfikatu powinien przesłać sprawozdanie z oceny do jednostki certyfikującej, która z kolei powinna poinformować krajowy organ ds. certyfikacji cyberbezpieczeństwa. Sprawozdanie powinno zawierać informacje na temat skutków podatności, niezbędnych zmian lub rozwiązań naprawczych, które są wymagane, w tym możliwych szerszych skutków podatności, a także rozwiązań naprawczych dotyczących innych produktów. W stosownych przypadkach procedurę ujawniania podatności powinna uzupełniać norma EN ISO/IEC 29147.

(27) Do celów certyfikacji jednostki oceniające zgodność i krajowe organy ds. certyfikacji cyberbezpieczeństwa uzyskują poufne i wrażliwe dane oraz tajemnice handlowe, również dotyczące własności intelektualnej lub monitorowania zgodności, które wymagają odpowiedniej ochrony. Powinny one zatem posiadać niezbędne kompetencje techniczne i wiedzę techniczną oraz ustanowić systemy ochrony informacji. Wymogi i warunki ochrony informacji powinny być spełnione zarówno w odniesieniu do akredytacji, jak i zezwolenia.

(28) ENISA powinna udostępnić wykaz certyfikowanych profili zabezpieczeń na swojej stronie internetowej poświęconej certyfikacji cyberbezpieczeństwa i wskazywać ich status zgodnie z rozporządzeniem (UE) 2019/881.

(29) W niniejszym rozporządzeniu określa się warunki dotyczące umów o wzajemnym uznawaniu z państwami trzecimi. Takie umowy o wzajemnym uznawaniu mogą mieć charakter dwu- lub wielostronny i powinny zastąpić podobne obecnie obowiązujące umowy. W celu ułatwienia płynnego przejścia do takich umów o wzajemnym uznawaniu państwa członkowskie mogą przez ograniczony okres kontynuować istniejące porozumienia o współpracy z państwami trzecimi.

(30) Jednostki certyfikujące wydające certyfikaty EUCC o poziomie uzasadnienia zaufania „wysoki", a także odpowiednie powiązane ITSEF powinny być poddawane wzajemnej ocenie. Celem wzajemnych ocen powinno być ustalenie, czy struktura i procedury jednostki certyfikującej poddanej wzajemnej ocenie dalej spełniają wymogi programu EUCC. Wzajemne oceny różnią się od wzajemnych ocen przeprowadzanych przez krajowe organy ds. certyfikacji cyberbezpieczeństwa, jak przewidziano w art. 59 rozporządzenia (UE) 2019/881. Wzajemne oceny powinny służyć upewnieniu się, że jednostki certyfikujące działają w sposób zharmonizowany i wydają certyfikaty tej samej jakości, oraz powinny służyć zidentyfikowaniu wszelkich potencjalnych mocnych lub słabych stron w funkcjonowaniu jednostek certyfikujących, również z myślą o wymianie najlepszych praktyk. Ponieważ istnieją różne rodzaje jednostek certyfikujących, należy dopuścić różne rodzaje wzajemnej oceny. W bardziej złożonych przypadkach, jak na przykład w odniesieniu do jednostek certyfikujących wydających certyfikaty na różnych poziomach AVA_VAN, można stosować różne rodzaje wzajemnej oceny pod warunkiem spełnienia wszystkich wymogów.

(31) Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa powinna odgrywać ważną rolę w utrzymaniu programu. Działania te powinny być prowadzone między innymi w drodze współpracy z sektorem prywatnym, tworzenia wyspecjalizowanych podgrup oraz odpowiednich prac przygotowawczych i udzielania pomocy, o którą prosi Komisja. Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa odgrywa ważną rolę w zatwierdzaniu dokumentów odzwierciedlających stan wiedzy. Przy zatwierdzaniu i przyjmowaniu dokumentów odzwierciedlających stan wiedzy należy odpowiednio uwzględnić elementy, o których mowa w art. 54 ust. 1 lit. c) rozporządzenia (UE) 2019/881. Domeny techniczne powinny być publikowane w załączniku I do niniejszego rozporządzenia. Profile zabezpieczeń,

które przyjęto jako dokumenty odzwierciedlające stan wiedzy powinno być publikowane w załączniku II. Aby zapewnić dynamikę tych załączników, Komisja może je zmieniać – zgodnie z procedurą określoną w art. 66 ust. 2 rozporządzenia (UE) 2019/881 oraz z uwzględnieniem opinii Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa. Załącznik III zawiera zalecane profile zabezpieczeń, które w momencie wejścia w życie niniejszego rozporządzenia nie są dokumentami odzwierciedlającymi stan wiedzy. Powinny one być publikowane na stronie internetowej ENISA, o której mowa w art. 50 ust. 1 rozporządzenia (UE) 2019/881.

(32) Niniejsze rozporządzenie powinno stosować się od dnia przypadającego 12 miesięcy po jego wejściu w życie. Wymogi rozdziału IV i załącznika V nie wymagają okresu przejściowego i w związku z tym powinny mieć zastosowanie od dnia wejścia w życie niniejszego rozporządzenia.

(33) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią Europejskiego Komitetu ds. Certyfikacji Cyberbezpieczeństwa ustanowionego na mocy art. 66 rozporządzenia (UE) 2019/881,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

**PRZEPISY OGÓLNE**

*Artykuł 1*

**Przedmiot i zakres stosowania**

Niniejszym rozporządzeniem ustanawia się europejski program certyfikacji cyberbezpieczeństwa oparty na wspólnych kryteriach (EUCC).

Niniejsze rozporządzenie ma zastosowanie do wszystkich produktów technologii informacyjno-komunikacyjnych („ICT"), w tym ich dokumentacji, które są przedkładane do certyfikacji w ramach EUCC, oraz do wszystkich profili zabezpieczeń, które są przedkładane do certyfikacji w ramach procesu ICT prowadzącego do certyfikacji produktów ICT.

*Artykuł 2*

**Definicje**

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „wspólne kryteria" oznaczają wspólne kryteria oceny bezpieczeństwa technologii informacyjnych określone w normie ISO/IEC 15408;

2) „wspólna metodyka oceny" oznacza wspólną metodykę oceny bezpieczeństwa technologii informacyjnych określoną w normie ISO/IEC 18045;

3) „cel oceny" oznacza produkt ICT lub jego część lub profil zabezpieczeń stanowiący część procesu ICT, który podlega ocenie cyberbezpieczeństwa w celu uzyskania certyfikacji EUCC;

4) „cel bezpieczeństwa" oznacza twierdzenie dotyczące wymogów bezpieczeństwa zależnych od wdrożenia w odniesieniu do konkretnego produktu ICT;

5) „profil zabezpieczeń" oznacza proces ICT, który określa wymogi bezpieczeństwa dla określonej kategorii produktów ICT, przy uwzględnieniu niezależnych od wdrożenia potrzeb bezpieczeństwa, i który może być wykorzystywany do oceny produktów ICT należących do tej konkretnej kategorii na potrzeby ich certyfikacji;

6) „sprawozdanie techniczne z oceny” oznacza dokument sporządzony przez ITSEF w celu przedstawienia ustaleń, opinii i uzasadnień uzyskanych podczas oceny produktu ICT lub profilu zabezpieczeń zgodnie z zasadami i obowiązkami określonymi w niniejszym rozporządzeniu;

7) „ITSEF” oznacza jednostkę oceniającą bezpieczeństwo technologii informacyjnych, która jest jednostką oceniającą zgodność w rozumieniu art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, wykonującą zadania związane z oceną;

8) „poziom AVA_VAN” oznacza poziom analizy podatności uzasadnienia zaufania, który wskazuje stopień działań w zakresie oceny cyberbezpieczeństwa przeprowadzanych w celu określenia poziomu odporności na potencjalne wykorzystanie wad lub słabych stron celu oceny w jego środowisku operacyjnym, jak określono we wspólnych kryteriach;

9) „certyfikat EUCC” oznacza certyfikat cyberbezpieczeństwa wydany w ramach EUCC w odniesieniu do produktów ICT lub profili zabezpieczeń, które mogą być wykorzystywane wyłącznie w procesie ICT w zakresie certyfikacji produktów ICT;

10) „produkt złożony” oznacza produkt ICT oceniany wraz z innym bazowym produktem ICT, który otrzymał już certyfikat EUCC i na którego funkcji bezpieczeństwa polega złożony produkt ICT;

11) „krajowy organ ds. certyfikacji cyberbezpieczeństwa” oznacza organ wyznaczony przez państwo członkowskie zgodnie z art. 58 ust. 1 rozporządzenia (UE) 2019/881;

12) „jednostka certyfikująca” oznacza jednostkę oceniającą zgodność w rozumieniu art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, która wykonuje działania w zakresie certyfikacji;

13) „domena techniczna” oznacza wspólne ramy techniczne związane z konkretną technologią na potrzeby zharmonizowanej certyfikacji wraz z zestawem charakterystycznych wymogów bezpieczeństwa;

14) „dokument odzwierciedlający stan wiedzy” oznacza dokument, który określa metody, techniki i narzędzia oceny mające zastosowanie do certyfikacji produktów ICT, lub wymogi bezpieczeństwa generycznej kategorii produktów ICT, lub jakiekolwiek inne wymogi niezbędne do certyfikacji, w celu harmonizacji oceny, w szczególności w odniesieniu do domen technicznych lub profili zabezpieczeń;

15) „organ nadzoru rynku” oznacza organ zdefiniowany w art. 3 pkt 4 rozporządzenia (UE) 2019/1020.

*Artykuł 3*

**Normy oceny**

Do ocen przeprowadzanych w ramach programu EUCC zastosowanie mają następujące normy:

a) wspólne kryteria;

b) wspólna metodyka oceny.

*Artykuł 4*

**Poziomy uzasadnienia zaufania**

1. Jednostki certyfikujące wydają certyfikaty EUCC o poziomie uzasadnienia zaufania „istotny” lub „wysoki”.

2. Certyfikaty EUCC o poziomie uzasadnienia zaufania „istotny” odpowiadają certyfikatom, które obejmują poziom AVA_VAN 1 lub 2.

3. Certyfikaty EUCC o poziomie uzasadnienia zaufania „wysoki” odpowiadają certyfikatom, które obejmują poziom AVA_VAN 3, 4 lub 5.

4. Poziom uzasadnienia zaufania potwierdzony w certyfikacie EUCC umożliwia rozróżnienie między zgodnym i rozszerzonym wykorzystaniem komponentów uzasadnienia zaufania określonych we wspólnych kryteriach zgodnie z załącznikiem VIII.

5. Jednostki oceniające zgodność stosują te komponenty uzasadnienia zaufania, od których zależy wybrany poziom AVA_VAN, zgodnie z normami, o których mowa w art. 3.

*Artykuł 5*

**Metody certyfikacji produktów ICT**

1. Certyfikację produktu ICT przeprowadza się w odniesieniu do jego celu bezpieczeństwa:

a) określonego przez wnioskodawcę; lub

b) przez włączenie certyfikowanego profilu zabezpieczeń do procesu ICT, w przypadku gdy produkt ICT należy do kategorii produktów ICT objętej tym profilem zabezpieczeń.

2. Profile zabezpieczeń są certyfikowane wyłącznie do celów certyfikacji produktów ICT należących do określonej kategorii produktów ICT objętych danym profilem zabezpieczeń.

*Artykuł 6*

**Ocena zgodności przez stronę pierwszą**

Nie zezwala się na ocenę zgodności przez stronę pierwszą w rozumieniu art. 53 rozporządzenia (UE) 2019/881.

ROZDZIAŁ II

**CERTYFIKACJA PRODUKTÓW ICT**

*SEKCJA I*

***SZCZEGÓŁOWE NORMY I WYMOGI DOTYCZĄCE OCENY***

*Artykuł 7*

**Kryteria i metody oceny produktów ICT**

1. Produkt ICT przedłożony do certyfikacji ocenia się co najmniej zgodnie z następującymi zasadami:

a) mającymi zastosowanie elementami norm, o których mowa w art. 3;

b) klasami wymogów uzasadnienia zaufania do bezpieczeństwa na potrzeby oceny podatności oraz niezależnych badań funkcjonalnych, jak określono w normach oceny, o których mowa w art. 3;

c) poziomem ryzyka związanego z przewidzianym stosowaniem danych produktów ICT zgodnie z art. 52 rozporządzenia (UE) 2019/881 oraz ich funkcjami bezpieczeństwa wspierającymi cele bezpieczeństwa określone w art. 51 rozporządzenia (UE) 2019/881;

d) mającymi zastosowanie dokumentami odzwierciedlającymi stan wiedzy wymienionymi w załączniku I; oraz

e) mającymi zastosowanie certyfikowanymi profilami zabezpieczeń wymienionymi w załączniku II.

2. W wyjątkowych i należycie uzasadnionych przypadkach jednostka oceniająca zgodność może wnieść o zrezygnowanie z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy. W takich przypadkach jednostka oceniająca zgodność informuje krajowy organ ds. certyfikacji cyberbezpieczeństwa, podając należyte uzasadnienie swojego wniosku. Krajowy organ ds. certyfikacji cyberbezpieczeństwa ocenia uzasadnienie zastosowania wyjątku i, w uzasadnionych przypadkach, zatwierdza go. Do czasu podjęcia decyzji przez krajowy organ ds. certyfikacji cyberbezpieczeństwa jednostka

oceniająca zgodność nie wydaje żadnego certyfikatu. Krajowy organ ds. certyfikacji cyberbezpieczeństwa bez zbędnej zwłoki powiadamia o zatwierdzeniu wyjątku Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa, która może wydać opinię. Krajowy organ ds. certyfikacji cyberbezpieczeństwa w jak największym stopniu uwzględnia opinię Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa.

3. Certyfikacja produktów ICT na poziomie AVA_VAN 4 lub 5 jest możliwa wyłącznie w następujących scenariuszach:

a) w przypadku gdy produkt ICT jest objęty jakąkolwiek domeną techniczną wymienioną w załączniku I, ocenia się go zgodnie z mającymi zastosowanie dokumentami odzwierciedlającymi stan wiedzy właściwymi dla tych domen,

b) w przypadku gdy produkt ICT należy do kategorii produktów ICT objętych certyfikowanym profilem zabezpieczeń, który obejmuje poziom AVA_VAN 4 lub 5 i który wymieniono w załączniku II jako profil zabezpieczeń odzwierciedlającymi stan wiedzy, ocenia się go zgodnie z metodyką oceny określoną dla tego profilu zabezpieczeń,

c) w przypadku gdy lit. a) i b) niniejszego ustępu nie mają zastosowania, a włączenie domeny technicznej do załącznika I lub certyfikowanego profilu zabezpieczeń do załącznika II jest mało prawdopodobne w dającej się przewidzieć przyszłości, oraz wyłącznie w wyjątkowych i należycie uzasadnionych przypadkach, z zastrzeżeniem warunków określonych w ust. 4.

4. W przypadku gdy jednostka oceniająca zgodność uzna, że zachodzi wyjątkowy i należycie uzasadniony przypadek, o którym mowa w ust. 3 lit. c), powiadamia o zamierzonej certyfikacji krajowy organ ds. certyfikacji cyberbezpieczeństwa, podając uzasadnienie i proponowaną metodykę oceny. Krajowy organ ds. certyfikacji cyberbezpieczeństwa ocenia uzasadnienie zastosowania wyjątku i, w uzasadnionych przypadkach, zatwierdza lub zmienia metodykę oceny, która ma być stosowana przez jednostkę oceniającą zgodność. Do czasu podjęcia decyzji przez krajowy organ ds. certyfikacji cyberbezpieczeństwa jednostka oceniająca zgodność nie wydaje żadnego certyfikatu. Krajowy organ ds. certyfikacji cyberbezpieczeństwa bez zbędnej zwłoki zgłasza zamierzoną certyfikację Europejskiej Grupie ds. Certyfikacji Cyberbezpieczeństwa, która może wydać opinię. Krajowy organ ds. certyfikacji cyberbezpieczeństwa w jak największym stopniu uwzględnia opinię Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa.

5. W przypadku produktu ICT poddawanego ocenie produktu złożonego, zgodnie z odpowiednimi dokumentami odzwierciedlającymi stan wiedzy, ITSEF, która przeprowadziła ocenę bazowego produktu ICT, przekazuje odpowiednie informacje ITSEF przeprowadzającemu ocenę złożonego produktu ICT.

*Sekcja II*

***Wydawanie, odnawianie i cofanie certyfikatów EUCC***

*Artykuł 8*

**Informacje niezbędne do certyfikacji**

1. Wnioskodawca ubiegający się o certyfikację w ramach EUCC dostarcza lub w inny sposób udostępnia jednostce certyfikującej i ITSEF wszelkie informacje niezbędne do działań w zakresie certyfikacji.

2. Informacje, o których mowa w ust. 1, obejmują wszystkie istotne dowody zgodnie z sekcjami „Elementy działania twórcy" w odpowiednim formacie określonym w sekcjach „Treść i prezentacja elementu dowodu" wspólnych kryteriów i wspólnej metodyki oceny w odniesieniu do wybranego poziomu uzasadnienia zaufania i związanych z nim wymogów uzasadnienia zaufania do bezpieczeństwa. Dowody obejmują, w razie potrzeby, szczegółowe informacje na temat produktu ICT i jego kodu źródłowego zgodnie z niniejszym rozporządzeniem, z zastrzeżeniem zabezpieczeń przed nieuprawnionym ujawnieniem.

3. Wnioskodawcy ubiegający się o certyfikację mogą przedstawić jednostce certyfikującej i ITSEF odpowiednie wyniki oceny z wcześniejszej certyfikacji zgodnie z:

a) niniejszym rozporządzeniem;

b) innym europejskim programem certyfikacji cyberbezpieczeństwa przyjętym na podstawie art. 49 rozporządzenia (UE) 2019/881;

c) programem krajowym, o którym mowa w art. 49 niniejszego rozporządzenia.

4. W przypadku gdy wyniki oceny są istotne dla zadań ITSEF, jednostka ta może ponownie wykorzystać wyniki oceny, pod warunkiem że wyniki te są zgodne z obowiązującymi wymogami, a ich autentyczność jest potwierdzona.

5. W przypadku gdy jednostka certyfikująca zezwala na poddanie produktu certyfikacji produktu złożonego, wnioskodawca ubiegający się o certyfikację udostępnia jednostce certyfikującej i ITSEF wszystkie niezbędne elementy, w stosownych przypadkach, zgodnie z dokumentem odzwierciedlającym stan wiedzy.

6. Wnioskodawcy ubiegający się o certyfikację przekazują również jednostce certyfikującej i ITSEF następujące informacje:

a) link do swojej strony internetowej zawierającej dodatkowe informacje na temat cyberbezpieczeństwa, o których mowa w art. 55 rozporządzenia (UE) 2019/881;

b) opis stosowanych przez wnioskodawcę procedur zarządzania podatnościami i ujawniania podatności.

7. Cała odpowiednia dokumentacja, o której mowa w niniejszym artykule, jest przechowywana przez jednostkę certyfikującą, ITSEF i wnioskodawcę przez 5 lat po wygaśnięciu certyfikatu.

*Artykuł 9*

**Warunki wydania certyfikatu EUCC**

1. Jednostki certyfikujące wydają certyfikat EUCC, jeżeli spełnione są wszystkie następujące warunki:

a) kategoria produktu ICT wchodzi w zakres akredytacji, a w stosownych przypadkach zezwolenia, jednostki certyfikującej i ITSEF zaangażowanych w certyfikację;

b) wnioskodawca ubiegający się o certyfikację podpisał oświadczenie zawierające wszystkie zobowiązania wymienione w ust. 2;

c) ITSEF zakończyła ocenę bez zastrzeżeń zgodnie z normami, kryteriami i metodami oceny, o których mowa w art. 3 i 7;

d) jednostka certyfikująca zakończyła przegląd wyników oceny bez zastrzeżeń;

e) jednostka certyfikująca zweryfikowała, że sprawozdania techniczne z oceny przedstawione przez ITSEF są zgodne z przedstawionymi dowodami oraz że normy, kryteria i metody oceny, o których mowa w art. 3 i 7, zastosowano prawidłowo.

2. Wnioskodawca ubiegający się o certyfikację zobowiązuje się:

a) dostarczyć jednostce certyfikującej i ITSEF wszelkie niezbędne kompletne i prawidłowe informacje, a na żądanie dostarczyć dodatkowe niezbędne informacje;

b) nie promować produktu ICT jako certyfikowanego w ramach EUCC, zanim certyfikat EUCC nie zostanie wydany;

c) promować produkt ICT jako certyfikowany wyłącznie w odniesieniu do zakresu określonego w certyfikacie EUCC;

d) natychmiast zaprzestać promowania produktu ICT jako certyfikowanego w przypadku zawieszenia, cofnięcia lub wygaśnięcia certyfikatu EUCC;

e) zapewnić, aby produkty ICT sprzedawane z odniesieniem do certyfikatu EUCC były ściśle identyczne z produktem ICT poddanym certyfikacji;

f) przestrzegać zasad używania znaku i etykiety ustanowionych dla certyfikatu EUCC zgodnie z art. 11.

3. W przypadku produktu ICT poddawanego certyfikacji produktu złożonego, zgodnie z odpowiednimi dokumentami odzwierciedlającymi stan wiedzy, jednostka certyfikująca, która przeprowadziła certyfikację bazowego produktu ICT, przekazuje odpowiednie informacje jednostce certyfikującej przeprowadzającej certyfikację złożonego produktu ICT.

*Artykuł 10*

**Treść i format certyfikatu EUCC**

1. Certyfikat EUCC zawiera co najmniej informacje określone w załączniku VII.

2. Zakres i granice certyfikowanego produktu ICT określa się jednoznacznie w certyfikacie EUCC lub sprawozdaniu z certyfikacji, wskazując, czy certyfikowano cały produkt ICT, czy tylko jego części.

3. Jednostka certyfikująca przekazuje wnioskodawcy certyfikat EUCC co najmniej w formie elektronicznej.

4. Jednostka certyfikująca sporządza sprawozdanie z certyfikacji zgodnie z załącznikiem V dla każdego wydanego przez siebie certyfikatu EUCC. Sprawozdanie z certyfikacji opiera się na sprawozdaniu technicznym z oceny wydanym przez ITSEF. W sprawozdaniu technicznym z oceny i sprawozdaniu z certyfikacji wskazuje się szczegółowe kryteria i metody oceny, o których mowa w art. 7, zastosowane na potrzeby oceny.

5. Jednostka certyfikująca przekazuje krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i ENISA każdy certyfikat EUCC i każde sprawozdanie z certyfikacji w formie elektronicznej.

*Artykuł 11*

**Znak i etykieta**

1. Posiadacz certyfikatu może na certyfikowanym produkcie ICT umieścić znak i etykietę. Znak i etykieta wskazują, że produkt ICT certyfikowano zgodnie z niniejszym rozporządzeniem. Znak i etykietę umieszcza się zgodnie z niniejszym artykułem i załącznikiem IX.

2. Znak i etykietę umieszcza się na certyfikowanym produkcie ICT lub jego tabliczce znamionowej w sposób widoczny, czytelny i trwały. W przypadku gdy nie jest to możliwe lub nie jest to uzasadnione z uwagi na charakter produktu, umieszcza się je na opakowaniu oraz w dokumentach towarzyszących produktowi. W przypadku gdy certyfikowany produkt ICT dostarczany jest w formie oprogramowania, znak i etykietę umieszcza się w sposób widoczny, czytelny i trwały w dokumentacji towarzyszącej lub dokumentacja ta musi być łatwo i bezpośrednio dostępna dla użytkowników za pośrednictwem strony internetowej.

3. Znak i etykieta są określone w załączniku IX i zawierają:

a) poziom uzasadnienia zaufania i poziom AVA_VAN certyfikowanego produktu ICT;

b) niepowtarzalny identyfikator certyfikatu, składający się z:

   1) nazwy programu;

   2) nazwy i numeru referencyjnego akredytacji jednostki certyfikującej, która wydała certyfikat;

   3) roku i miesiąca wydania;

   4) numeru identyfikacyjnego przydzielonego przez jednostkę certyfikującą, która wydała certyfikat.

4. Znakowi i etykiecie towarzyszy kod QR wraz z linkiem do strony internetowej zawierającej co najmniej:

a) informacje na temat ważności certyfikatu;

b) niezbędne informacje dotyczące certyfikacji określone w załącznikach V i VII;

c) informacje, które posiadacz certyfikatu ma udostępniać publicznie zgodnie z art. 55 rozporządzenia (UE) 2019/881; oraz

d) w stosownych przypadkach – informacje historyczne związane z konkretną certyfikacją lub konkretnymi certyfikacjami produktu ICT w celu umożliwienia identyfikowalności.

*Artykuł 12*

**Okres ważności certyfikatu EUCC**

1. Jednostka certyfikująca ustala okres ważności każdego wydanego certyfikatu EUCC, uwzględniając charakterystykę certyfikowanego produktu ICT.

2. Okres ważności certyfikatu EUCC nie może przekraczać 5 lat.

3. Na zasadzie odstępstwa od ust. 2 okres ten może przekraczać 5 lat, pod warunkiem uzyskania uprzedniej zgody krajowego organu ds. certyfikacji cyberbezpieczeństwa. Krajowy organ ds. certyfikacji cyberbezpieczeństwa bez zbędnej zwłoki powiadamia Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa o udzielonej zgodzie.

*Artykuł 13*

**Przegląd certyfikatu EUCC**

1. Na wniosek posiadacza certyfikatu lub z innych uzasadnionych powodów jednostka certyfikująca może podjąć decyzję o przeglądzie certyfikatu EUCC dla produktu ICT. Przegląd przeprowadza się zgodnie z załącznikiem IV. Jednostka certyfikująca określa zakres przeglądu. Jeżeli jest to konieczne do przeprowadzenia przeglądu, jednostka certyfikująca zwraca się do ITSEF o przeprowadzenie ponownej oceny certyfikowanego produktu ICT.

2. Po uzyskaniu wyników przeglądu oraz, w stosownych przypadkach, ponownej oceny jednostka certyfikująca:

a) potwierdza certyfikat EUCC;

b) cofa certyfikat EUCC zgodnie z art. 14;

c) cofa certyfikat EUCC zgodnie z art. 14 i wydaje nowy certyfikat EUCC o identycznym zakresie i przedłużonym okresie ważności; albo

d) cofa certyfikat EUCC zgodnie z art. 14 i wydaje nowy certyfikat EUCC o innym zakresie.

3. Jednostka certyfikująca może podjąć decyzję o zawieszeniu, bez zbędnej zwłoki, certyfikatu EUCC zgodnie z art. 30 do czasu podjęcia działań zaradczych przez posiadacza certyfikatu EUCC.

*Artykuł 14*

**Cofnięcie certyfikatu EUCC**

1. Bez uszczerbku dla art. 58 ust. 8 lit. e) rozporządzenia (UE) 2019/881 certyfikat EUCC cofa jednostka certyfikująca, która wydała ten certyfikat.

2. Jednostka certyfikująca, o której mowa w ust. 1, powiadamia krajowy organ ds. certyfikacji cyberbezpieczeństwa o cofnięciu certyfikatu. Powiadamia ona również ENISA o takim cofnięciu, aby ułatwić jej wykonywanie zadań na podstawie art. 50 rozporządzenia (UE) 2019/881. Krajowy organ ds. certyfikacji cyberbezpieczeństwa powiadamia inne właściwe organy nadzoru rynku.

3. Posiadacz certyfikatu EUCC może wystąpić o jego cofnięcie.

ROZDZIAŁ III

**CERTYFIKACJA PROFILI ZABEZPIECZEŃ**

*SEKCJA I*

***SZCZEGÓŁOWE NORMY I WYMOGI DOTYCZĄCE OCENY***

*Artykuł 15*

**Kryteria i metody oceny**

1. Profil zabezpieczeń ocenia się co najmniej zgodnie z następującymi zasadami:

a) mającymi zastosowanie elementami norm, o których mowa w art. 3;

b) poziomem ryzyka związanego z przewidzianym stosowaniem danych produktów ICT zgodnie z art. 52 rozporządzenia (UE) 2019/881 oraz ich funkcjami bezpieczeństwa wspierającymi cele bezpieczeństwa określone w art. 51 tego rozporządzenia; oraz

c) mającymi zastosowanie dokumentami odzwierciedlającymi stan wiedzy wymienionymi w załączniku I. Profil zabezpieczeń objęty domeną techniczną certyfikuje się zgodnie z wymogami określonymi w tej domenie technicznej.

2. W wyjątkowych i należycie uzasadnionych przypadkach jednostka oceniająca zgodność może certyfikować profil zabezpieczeń bez zastosowania odpowiednich dokumentów odzwierciedlających stan wiedzy. W takich przypadkach informuje ona o tym właściwy krajowy organ ds. certyfikacji cyberbezpieczeństwa i przedstawia uzasadnienie zamierzonej certyfikacji bez zastosowania odpowiednich dokumentów odzwierciedlających stan wiedzy oraz proponowaną metodykę oceny. Krajowy organ ds. certyfikacji cyberbezpieczeństwa ocenia to uzasadnienie i, w uzasadnionych przypadkach, zatwierdza zrezygnowanie z zastosowania odpowiednich dokumentów odzwierciedlających stan wiedzy oraz zatwierdza lub zmienia, w stosownych przypadkach, metodykę oceny, która ma być stosowana przez jednostkę oceniającą zgodność. Do czasu podjęcia decyzji przez krajowy organ ds. certyfikacji cyberbezpieczeństwa jednostka oceniająca zgodność nie wydaje żadnego certyfikatu w odniesieniu do danego profilu zabezpieczeń. Krajowy organ ds. certyfikacji cyberbezpieczeństwa bez zbędnej zwłoki powiadamia o zatwierdzonym zrezygnowaniu z zastosowania odpowiednich dokumentów odzwierciedlających stan wiedzy Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa, która może wydać opinię. Krajowy organ ds. certyfikacji cyberbezpieczeństwa w jak największym stopniu uwzględnia opinię Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa.

*SEKCJA II*

***WYDAWANIE, ODNAWIANIE I COFANIE CERTYFIKATÓW EUCC DLA PROFILI ZABEZPIECZEŃ***

*Artykuł 16*

**Informacje niezbędne do certyfikacji profili zabezpieczeń**

Wnioskodawca ubiegający się o certyfikację profilu zabezpieczeń dostarcza lub w inny sposób udostępnia jednostce certyfikującej i ITSEF wszelkie informacje niezbędne do działań w zakresie certyfikacji. Art. 8 ust. 2, 3, 4 i 7 stosuje się odpowiednio.

*Artykuł 17*

**Wydawanie certyfikatów EUCC dla profili zabezpieczeń**

1. Wnioskodawca ubiegający się o certyfikację dostarcza jednostce certyfikującej i ITSEF wszelkie niezbędne kompletne i prawidłowe informacje.

2. Art. 9 i 10 stosuje się odpowiednio.

3. ITSEF ocenia, czy profil zabezpieczeń jest kompletny, spójny, solidny pod względem technicznym i skuteczny w odniesieniu do przewidzianego stosowania i celów bezpieczeństwa kategorii produktu ICT objętej tym profilem zabezpieczeń.

4. Profil zabezpieczeń jest certyfikowany wyłącznie przez:

a) krajowy organ ds. certyfikacji cyberbezpieczeństwa lub inny podmiot publiczny akredytowany jako jednostka certyfikująca; lub

b) jednostkę certyfikującą, po uprzednim zatwierdzeniu przez krajowy organ ds. certyfikacji cyberbezpieczeństwa w odniesieniu do każdego indywidualnego profilu zabezpieczeń.

*Artykuł 18*

**Okres ważności certyfikatu EUCC dla profili zabezpieczeń**

1. Jednostka certyfikująca ustala okres ważności każdego certyfikatu EUCC.

2. Okres ważności może odpowiadać maksymalnie całemu cyklowi życia danego profilu zabezpieczeń.

*Artykuł 19*

**Przegląd certyfikatu EUCC dla profili zabezpieczeń**

1. Na wniosek posiadacza certyfikatu lub z innych uzasadnionych powodów jednostka certyfikująca może podjąć decyzję o przeglądzie certyfikatu EUCC dla profilu zabezpieczeń. Przegląd przeprowadza się z zastosowaniem warunków określonych w art. 15. Jednostka certyfikująca określa zakres przeglądu. Jeżeli jest to konieczne do przeprowadzenia przeglądu, jednostka certyfikująca zwraca się do ITSEF o przeprowadzenie ponownej oceny certyfikowanego profilu zabezpieczeń.

2. Po uzyskaniu wyników przeglądu oraz, w stosownych przypadkach, ponownej oceny jednostka certyfikująca wykonuje jedną z następujących czynności:

a) potwierdza certyfikat EUCC;

b) cofa certyfikat EUCC zgodnie z art. 20;

c) cofa certyfikat EUCC zgodnie z art. 20 i wydaje nowy certyfikat EUCC o identycznym zakresie i przedłużonym okresie ważności;

d) cofa certyfikat EUCC zgodnie z art. 20 i wydaje nowy certyfikat EUCC o innym zakresie.

*Artykuł 20*

**Cofnięcie certyfikatu EUCC dla profilu zabezpieczeń**

1. Bez uszczerbku dla art. 58 ust. 8 lit. e) rozporządzenia (UE) 2019/881 certyfikat EUCC dla profilu zabezpieczeń cofa jednostka certyfikująca, która wydała ten certyfikat. Art. 14 stosuje się odpowiednio.

2. Certyfikat dla profilu zabezpieczeń wydany zgodnie z art. 17 ust. 4 lit. b) cofa krajowy organ ds. certyfikacji cyberbezpieczeństwa, który zatwierdził ten certyfikat.

ROZDZIAŁ IV

**JEDNOSTKI OCENIAJĄCE ZGODNOŚĆ**

*Artykuł 21*

**Dodatkowe lub szczególne wymogi obowiązujące jednostkę certyfikującą**

1. Jednostka certyfikująca ma zezwolenie krajowego organu ds. certyfikacji cyberbezpieczeństwa na wydawanie certyfikatów EUCC o poziomie uzasadnienia zaufania „wysoki", jeżeli oprócz spełnienia wymogów określonych w art. 60 ust. 1 rozporządzenia (UE) 2019/881 i w załączniku do tego rozporządzenia, dotyczących akredytacji jednostek oceniających zgodność, jednostka ta wykaże, że:

a) dysponuje wiedzą fachową i kompetencjami wymaganymi do podjęcia decyzji w sprawie certyfikacji o poziomie uzasadnienia zaufania „wysoki";

b) prowadzi działania w zakresie certyfikacji we współpracy z ITSEF upoważnioną zgodnie z art. 22; oraz

c) dysponuje niezbędnymi kompetencjami i wprowadziła odpowiednie środki techniczne i operacyjne w celu skutecznej ochrony informacji poufnych i szczególnie chronionych na potrzeby poziomu uzasadnienia zaufania „wysoki", oprócz wymogów określonych w art. 43.

2. Krajowy organ ds. certyfikacji cyberbezpieczeństwa ocenia, czy jednostka certyfikująca spełnia wszystkie wymogi określone w ust. 1. Ocena ta obejmuje co najmniej ustrukturyzowane wywiady oraz przegląd co najmniej jednej certyfikacji pilotażowej przeprowadzonej przez jednostkę certyfikującą zgodnie z niniejszym rozporządzeniem.

W swojej ocenie krajowy organ ds. certyfikacji cyberbezpieczeństwa może ponownie wykorzystać wszelkie odpowiednie dowody pochodzące z uprzedniego zezwolenia, lub podobnych działań, udzielonego zgodnie z:

a) niniejszym rozporządzeniem;

b) innym europejskim programem certyfikacji cyberbezpieczeństwa przyjętym na podstawie art. 49 rozporządzenia (UE) 2019/881;

c) programem krajowym, o którym mowa w art. 49 niniejszego rozporządzenia.

3. Krajowy organ ds. certyfikacji cyberbezpieczeństwa sporządza sprawozdanie dotyczące zezwolenia, które podlega wzajemnemu przeglądowi zgodnie z art. 59 ust. 3 lit. d) rozporządzenia (UE) 2019/881.

4. Krajowy organ ds. certyfikacji cyberbezpieczeństwa określa kategorie produktów ICT i profile zabezpieczeń, które obejmuje zezwolenie. Zezwolenie jest ważne przez okres nie dłuższy niż okres ważności akredytacji. Może ono zostać odnowione na wniosek, pod warunkiem że jednostka certyfikująca nadal spełnia wymogi określone w niniejszym artykule. W celu odnowienia zezwolenia nie są wymagane żadne oceny pilotażowe.

5. Krajowy organ ds. certyfikacji cyberbezpieczeństwa cofa zezwolenie dla jednostki certyfikującej, jeżeli przestała ona spełniać warunki określone w niniejszym artykule. Po cofnięciu zezwolenia jednostka certyfikująca zaprzestaje natychmiast promowania się jako jednostka certyfikująca posiadająca zezwolenie.

*Artykuł 22*

**Dodatkowe lub szczególne wymogi obowiązujące ITSEF**

1. ITSEF ma zezwolenie krajowego organu ds. certyfikacji cyberbezpieczeństwa na przeprowadzanie oceny produktów ICT podlegających certyfikacji na poziomie uzasadnienia zaufania „wysoki", jeżeli oprócz spełnienia wymogów określonych w art. 60 ust. 1 rozporządzenia (UE) 2019/881 i w załączniku do tego rozporządzenia, dotyczących akredytacji jednostek oceniających zgodność, ITSEF wykaże, że spełnia wszystkie następujące warunki:

a) dysponuje wiedzą fachową niezbędną do przeprowadzania działań w zakresie oceny w celu określenia odporności na zaawansowane cyberataki przeprowadzane przez podmioty o znacznych umiejętnościach i zasobach;

b) w odniesieniu do domen technicznych i profili zabezpieczeń, które są częścią procesu ICT dla tych produktów ICT, dysponuje:

1) wiedzą fachową umożliwiającą przeprowadzenie konkretnych działań w zakresie oceny niezbędnych do metodycznego określenia odporności celu oceny na zaawansowane ataki w jego środowisku operacyjnym, przy założeniu potencjału ataku „umiarkowany" lub „wysoki", jak określono w normach, o których mowa w art. 3;

2) kompetencjami technicznymi określonymi w dokumentach odzwierciedlających stan wiedzy wymienionych w załączniku I;

c) dysponuje niezbędnymi kompetencjami i wprowadziła odpowiednie środki techniczne i operacyjne w celu skutecznej ochrony informacji poufnych i szczególnie chronionych na potrzeby poziomu uzasadnienia zaufania „wysoki", oprócz wymogów określonych w art. 43.

2. Krajowy organ ds. certyfikacji cyberbezpieczeństwa ocenia, czy ITSEF spełnia wszystkie wymogi określone w ust. 1. Ocena ta obejmuje co najmniej ustrukturyzowane wywiady oraz przegląd co najmniej jednej oceny pilotażowej przeprowadzonej przez ITSEF zgodnie z niniejszym rozporządzeniem.

3. W swojej ocenie krajowy organ ds. certyfikacji cyberbezpieczeństwa może ponownie wykorzystać wszelkie odpowiednie dowody pochodzące z uprzedniego zezwolenia, lub podobnych działań, udzielonego zgodnie z:

a) niniejszym rozporządzeniem;

b) innym europejskim programem certyfikacji cyberbezpieczeństwa przyjętym na podstawie art. 49 rozporządzenia (UE) 2019/881;

c) programem krajowym, o którym mowa w art. 49 niniejszego rozporządzenia.

4. Krajowy organ ds. certyfikacji cyberbezpieczeństwa sporządza sprawozdanie dotyczące zezwolenia, które podlega wzajemnemu przeglądowi zgodnie z art. 59 ust. 3 lit. d) rozporządzenia (UE) 2019/881.

5. Krajowy organ ds. certyfikacji cyberbezpieczeństwa określa kategorie produktów ICT i profile zabezpieczeń, które obejmuje zezwolenie. Zezwolenie jest ważne przez okres nie dłuższy niż okres ważności akredytacji. Może ono zostać odnowione na wniosek, pod warunkiem że ITSEF nadal spełnia wymogi określone w niniejszym artykule. W celu odnowienia zezwolenia nie powinny być wymagane żadne oceny pilotażowe.

6. Krajowy organ ds. certyfikacji cyberbezpieczeństwa cofa zezwolenie dla ITSEF, jeżeli przestała ona spełniać warunki określone w niniejszym artykule. Po cofnięciu zezwolenia ITSEF zaprzestaje promowania się jako ITSEF posiadająca zezwolenie.

*Artykuł 23*

**Notyfikacja jednostek certyfikujących**

1. Krajowy organ ds. certyfikacji cyberbezpieczeństwa notyfikuje Komisji jednostki certyfikujące na swoim terytorium, które są właściwe do certyfikacji na poziomie uzasadnienia zaufania „istotny" na podstawie ich akredytacji.

2. Krajowy organ ds. certyfikacji cyberbezpieczeństwa notyfikuje Komisji jednostki certyfikujące na swoim terytorium, które są właściwe do certyfikacji na poziomie uzasadnienia zaufania „wysoki" na podstawie ich akredytacji i decyzji o zezwoleniu.

3. Notyfikując Komisji jednostki certyfikujące, krajowy organ ds. certyfikacji cyberbezpieczeństwa przekazuje co najmniej następujące informacje:

a) poziom lub poziomy uzasadnienia zaufania, w odniesieniu do których jednostka certyfikująca jest właściwa do wydawania certyfikatów EUCC;

b) następujące informacje dotyczące akredytacji:

1) data akredytacji;

2) nazwa i adres jednostki certyfikującej;

3) państwo rejestracji jednostki certyfikującej;

4) numer referencyjny akredytacji;

5) zakres i okres ważności akredytacji;

6) adres, lokalizacja i link do odpowiedniej strony internetowej krajowej jednostki akredytującej; oraz

c) następujące informacje dotyczące zezwolenia w odniesieniu do poziomu „wysoki":

1) data udzielenia zezwolenia;

2) numer referencyjny zezwolenia;

3) okres ważności zezwolenia;

4) zakres zezwolenia, w tym najwyższy poziom AVA_VAN oraz, w stosownych przypadkach, objęta nim domena techniczna.

4. Krajowy organ ds. certyfikacji cyberbezpieczeństwa przesyła ENISA kopię notyfikacji, o której mowa w ust. 1 i 2, w celu opublikowania na stronie internetowej poświęconej certyfikacji cyberbezpieczeństwa dokładnych informacji na temat kwalifikowalności jednostek certyfikujących.

5. Krajowy organ ds. certyfikacji cyberbezpieczeństwa bez zbędnej zwłoki analizuje wszelkie informacje dotyczące zmiany statusu akredytacji przekazane przez krajową jednostkę akredytującą. W przypadku cofnięcia akredytacji lub zezwolenia krajowy organ ds. certyfikacji cyberbezpieczeństwa informuje o tym Komisję i może przedłożyć Komisji wniosek zgodnie z art. 61 ust. 4 rozporządzenia (UE) 2019/881.

*Artykuł 24*

**Notyfikacja ITSEF**

Określone w art. 23 obowiązki w zakresie notyfikacji dokonywanej przez krajowe organy ds. certyfikacji cyberbezpieczeństwa mają zastosowanie również do ITSEF. W notyfikacji podaje się adres ITSEF, ważną akredytację oraz, w stosownych przypadkach, ważne zezwolenie udzielone tej ITSEF.

ROZDZIAŁ V

**MONITOROWANIE, NIEZGODNOŚĆ I NIEPRZESTRZEGANIE PRZEPISÓW**

*SEKCJA I*

***MONITOROWANIE ZGODNOŚCI***

*Artykuł 25*

**Działania monitorujące prowadzone przez krajowy organ ds. certyfikacji cyberbezpieczeństwa**

1. Bez uszczerbku dla art. 58 ust. 7 rozporządzenia (UE) 2019/881 krajowy organ ds. certyfikacji cyberbezpieczeństwa monitoruje:

a) wykonywanie przez jednostkę certyfikującą i ITSEF obowiązków spoczywających na nich na podstawie niniejszego rozporządzenia i rozporządzenia (UE) 2019/881;

b) wykonywanie przez posiadaczy certyfikatu EUCC obowiązków spoczywających na nich na podstawie niniejszego rozporządzenia i rozporządzenia (UE) 2019/881;

c) zgodność certyfikowanych produktów ICT z wymogami określonymi w EUCC;

d) uzasadnienie zaufania wyrażone w certyfikacie EUCC dotyczące zmieniającego się krajobrazu zagrożeń.

2. Krajowy organ ds. certyfikacji cyberbezpieczeństwa wykonuje swoje działania monitorujące w szczególności na podstawie:

a) informacji pochodzących od jednostek certyfikujących, krajowych jednostek akredytujących i odpowiednich organów nadzoru rynku;

b) informacji wynikających z kontroli i dochodzeń przeprowadzonych przez siebie lub przez inny organ;

c) kontroli wyrywkowych przeprowadzanych zgodnie z ust. 3;

d) otrzymanych skarg.

3. Krajowy organ ds. certyfikacji cyberbezpieczeństwa, we współpracy z innymi organami nadzoru rynku, corocznie poddaje kontroli wyrywkowej co najmniej 4 % certyfikatów EUCC zgodnie z oceną ryzyka. Na wniosek właściwego krajowego organu ds. certyfikacji cyberbezpieczeństwa i działając w jego imieniu, jednostki certyfikujące oraz, w razie potrzeby, ITSEF pomagają temu organowi w monitorowaniu zgodności.

4. Krajowy organ ds. certyfikacji cyberbezpieczeństwa wybiera próbę certyfikowanych produktów ICT, które mają zostać poddane kontroli, stosując obiektywne kryteria, w tym:

a) kategorię produktu;

b) poziomy uzasadnienia zaufania produktów;

c) posiadacza certyfikatu;

d) jednostkę certyfikującą oraz, w stosownych przypadkach, ITSEF będącą podwykonawcą;

e) wszelkie inne informacje przekazane organowi.

5. Krajowy organ ds. certyfikacji cyberbezpieczeństwa informuje posiadaczy certyfikatu EUCC o wybranych produktach ICT i kryteriach wyboru.

6. Jednostka certyfikująca, która certyfikowała produkt ICT objęty próbą, na wniosek krajowego organu ds. certyfikacji cyberbezpieczeństwa, z pomocą odpowiedniej ITSEF, przeprowadza dodatkowy przegląd zgodnie z procedurą określoną w sekcji IV.2 załącznika IV i informuje krajowy organ ds. certyfikacji cyberbezpieczeństwa o jego wynikach.

7. Jeżeli krajowy organ ds. certyfikacji cyberbezpieczeństwa ma wystarczające powody, by sądzić, że certyfikowany produkt ICT nie jest już zgodny z niniejszym rozporządzeniem lub z rozporządzeniem (UE) 2019/881, może przeprowadzić dochodzenia lub skorzystać z jakichkolwiek innych uprawnień w zakresie monitorowania określonych w art. 58 ust. 8 rozporządzenia (UE) 2019/881.

8. Krajowy organ ds. certyfikacji cyberbezpieczeństwa informuje zainteresowaną jednostkę certyfikującą i zainteresowaną ITSEF o toczących się dochodzeniach dotyczących wybranych produktów ICT.

9. Jeżeli krajowy organ ds. certyfikacji cyberbezpieczeństwa stwierdzi, że toczące się dochodzenie dotyczy produktów ICT certyfikowanych przez jednostki certyfikujące mające siedzibę w innych państwach członkowskich, informuje o tym krajowe organy ds. certyfikacji cyberbezpieczeństwa odpowiednich państw członkowskich na potrzeby współpracy w dochodzeniach w stosownych przypadkach. Ten krajowy organ ds. certyfikacji cyberbezpieczeństwa powiadamia również Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa o dochodzeniach transgranicznych i ich wynikach.

*Artykuł 26*

**Działania monitorujące prowadzone przez jednostkę certyfikującą**

1. Jednostka certyfikująca monitoruje:

a) wykonywanie przez posiadaczy certyfikatu obowiązków spoczywających na nich na podstawie niniejszego rozporządzenia i rozporządzenia (UE) 2019/881 w odniesieniu do certyfikatu EUCC wydanego przez jednostkę certyfikującą;

b) zgodność certyfikowanych przez nią produktów ICT z odpowiednimi wymogami bezpieczeństwa;

c) uzasadnienie zaufania wyrażone w certyfikowanych profilach zabezpieczeń.

2. Jednostka certyfikująca podejmuje działania monitorujące na podstawie:

a) informacji dostarczonych na podstawie zobowiązań wnioskodawcy ubiegającego się o certyfikację, o których mowa w art. 9 ust. 2;

b) informacji wynikających z działań innych właściwych organów nadzoru rynku;

c) otrzymanych skarg;

d) informacji o podatnościach, które mogą mieć wpływ na certyfikowane przez nią produkty ICT.

3. Krajowy organ ds. certyfikacji cyberbezpieczeństwa może opracować zasady okresowego dialogu między jednostkami certyfikującymi a posiadaczami certyfikatów EUCC na potrzeby weryfikacji i sprawozdawczości w zakresie wykonywania zobowiązań podjętych na podstawie art. 9 ust. 2, bez uszczerbku dla działań związanych z innymi właściwymi organami nadzoru rynku.

*Artykuł 27*

**Działania monitorujące prowadzone przez posiadacza certyfikatu**

1. Posiadacz certyfikatu EUCC wykonuje następujące zadania w celu monitorowania zgodności certyfikowanego produktu ICT z jego wymogami bezpieczeństwa:

a) monitoruje informacje o podatnościach w odniesieniu do certyfikowanego produktu ICT, w tym w odniesieniu do znanych zależności, za pomocą własnych środków, ale także z uwzględnieniem:

   1) publikacji lub informacji o podatnościach pochodzących od użytkownika lub eksperta w obszarze bezpieczeństwa, o których mowa w art. 55 ust. 1 lit. c) rozporządzenia (UE) 2019/881;

   2) informacji z jakiegokolwiek innego źródła;

b) monitoruje uzasadnienie zaufania wyrażone w certyfikacie EUCC.

2. Posiadacz certyfikatu EUCC współpracuje z jednostką certyfikującą, ITSEF oraz, w stosownych przypadkach, z krajowym organem ds. certyfikacji cyberbezpieczeństwa w celu wspierania ich działań monitorujących.

SEKCJA II

***ZGODNOŚĆ I PRZESTRZEGANIE PRZEPISÓW***

*Artykuł 28*

**Konsekwencje niezgodności certyfikowanego produktu ICT lub profilu zabezpieczeń**

1. W przypadku gdy certyfikowany produkt ICT lub profil zabezpieczeń jest niezgodny z wymogami określonymi w niniejszym rozporządzeniu i w rozporządzeniu (UE) 2019/881, jednostka certyfikująca informuje posiadacza certyfikatu EUCC o stwierdzonej niezgodności i zwraca się do niego o podjęcie działań zaradczych.

2. W przypadku gdy niezgodność z przepisami niniejszego rozporządzenia może mieć wpływ na zgodność z innymi odpowiednimi przepisami Unii, które przewidują możliwość wykazania domniemania zgodności z wymogami tego aktu prawnego za pomocą certyfikatu EUCC, jednostka certyfikująca niezwłocznie informuje o tym krajowy organ ds. certyfikacji cyberbezpieczeństwa. Krajowy organ ds. certyfikacji cyberbezpieczeństwa niezwłocznie powiadamia o stwierdzonym przypadku niezgodności organ nadzoru rynku odpowiedzialny za takie inne odpowiednie przepisy Unii.

3. Po otrzymaniu informacji, o których mowa w ust. 1, posiadacz certyfikatu EUCC w terminie wyznaczonym przez jednostkę certyfikującą, nieprzekraczającym 30 dni, proponuje jednostce certyfikującej działania zaradcze niezbędne do usunięcia niezgodności.

4. Jednostka certyfikująca może bez zbędnej zwłoki zawiesić certyfikat EUCC zgodnie z art. 30 w nagłych przypadkach lub jeżeli posiadacz certyfikatu EUCC nie współpracuje z nią należycie.

5. Jednostka certyfikująca przeprowadza przegląd zgodnie z art. 13 i 19, oceniając, czy działanie zaradcze rozwiązuje problem niezgodności.

6. Jeżeli posiadacz certyfikatu EUCC nie zaproponuje odpowiednich działań zaradczych w okresie, o którym mowa w ust. 3, certyfikat zostaje zawieszony zgodnie z art. 30 lub cofnięty zgodnie z art. 14 lub 20.

7. Niniejszy artykuł nie ma zastosowania do przypadków podatności mających wpływ na certyfikowany produkt ICT, które należy rozpatrywać zgodnie z rozdziałem VI.

*Artykuł 29*

**Konsekwencje nieprzestrzegania przepisów przez posiadacza certyfikatu**

1. Jeżeli jednostka certyfikująca stwierdzi, że:

a) posiadacz certyfikatu EUCC lub wnioskodawca ubiegający się o certyfikację nie wykonuje swoich zobowiązań i obowiązków określonych w art. 9 ust. 2, art. 17 ust. 2, art. 27 i 41; lub

b) posiadacz certyfikatu EUCC nie spełnia wymogów art. 56 ust. 8 rozporządzenia (UE) 2019/881 lub rozdziału VI niniejszego rozporządzenia;

wyznacza okres nie dłuższy niż 30 dni, w którym posiadacz certyfikatu EUCC musi podjąć działania zaradcze.

2. Jeżeli posiadacz certyfikatu EUCC nie zaproponuje odpowiednich działań zaradczych w okresie, o którym mowa w ust. 1, certyfikat zostaje zawieszony zgodnie z art. 30 lub cofnięty zgodnie z art. 14 i art. 20.

3. Ciągłe lub powtarzające się naruszanie przez posiadacza certyfikatu EUCC obowiązków, o których mowa w ust. 1, powoduje cofnięcie certyfikatu EUCC zgodnie z art. 14 lub art. 20.

4. Jednostka certyfikująca informuje krajowy organ ds. certyfikacji cyberbezpieczeństwa o ustaleniach, o których mowa w ust. 1. W przypadku gdy nieprzestrzeganie przepisów ma wpływ na zgodność z innymi odpowiednimi przepisami Unii, krajowy organ ds. certyfikacji cyberbezpieczeństwa niezwłocznie powiadamia o stwierdzonym przypadku nieprzestrzegania przepisów organ nadzoru rynku odpowiedzialny za takie inne odpowiednie przepisy Unii.

*Artykuł 30*

**Zawieszenie certyfikatu EUCC**

1. W przypadku gdy niniejsze rozporządzenie odnosi się do zawieszenia certyfikatu EUCC, jednostka certyfikująca zawiesza dany certyfikat EUCC na okres odpowiedni do okoliczności powodujących zawieszenie, nieprzekraczający 42 dni. Bieg okresu zawieszenia rozpoczyna się w dniu następującym po dniu podjęcia decyzji przez jednostkę certyfikującą. Zawieszenie nie wpływa na ważność certyfikatu.

2. Jednostka certyfikująca bez zbędnej zwłoki powiadamia posiadacza certyfikatu i krajowy organ ds. certyfikacji cyberbezpieczeństwa o zawieszeniu oraz podaje przyczyny zawieszenia, wymagane działania, które należy podjąć, oraz okres zawieszenia.

3. Posiadacze certyfikatów powiadamiają nabywców danych produktów ICT o zawieszeniu i powodach zawieszenia przedstawionych przez jednostkę certyfikującą, z wyjątkiem tych części powodów, których ujawnienie stanowiłoby ryzyko dla bezpieczeństwa lub które zawierają informacje szczególnie chronione. Posiadacz certyfikatu również udostępnia publicznie te informacje.

4. W przypadku gdy inne odpowiednie przepisy Unii przewidują domniemanie zgodności na podstawie certyfikatów wydanych zgodnie z przepisami niniejszego rozporządzenia, krajowy organ ds. certyfikacji cyberbezpieczeństwa informuje o zawieszeniu organ nadzoru rynku odpowiedzialny za takie inne odpowiednie przepisy Unii.

5. O zawieszeniu certyfikatu powiadamia się ENISA zgodnie z art. 42 ust. 3.

6. W należycie uzasadnionych przypadkach krajowy organ ds. certyfikacji cyberbezpieczeństwa może zezwolić na przedłużenie okresu zawieszenia certyfikatu EUCC. Całkowity okres zawieszenia nie może przekraczać jednego roku.

*Artykuł 31*

**Konsekwencje nieprzestrzegania przepisów przez jednostkę oceniającą zgodność**

1. W przypadku niewywiązywania się z obowiązków przez jednostkę certyfikującą lub przez odpowiednią jednostkę certyfikującą w razie stwierdzenia niewywiązywania się z obowiązków przez ITSEF krajowy organ ds. certyfikacji cyberbezpieczeństwa bez zbędnej zwłoki:

a) identyfikuje, przy wsparciu zainteresowanej ITSEF, certyfikaty EUCC, na które może to mieć wpływ;

b) w razie potrzeby zwraca się o przeprowadzenie działań w zakresie oceny przez ITSEF, który przeprowadził ocenę, albo jakąkolwiek inną akredytowaną i, w stosownych przypadkach, posiadającą zezwolenie ITSEF, która może być w lepszej sytuacji technicznej, aby wesprzeć tę identyfikację, w odniesieniu do co najmniej jednego produktu ICT lub profilu zabezpieczeń;

c) analizuje skutki nieprzestrzegania przepisów;

d) powiadamia o nieprzestrzeganiu przepisów posiadacza certyfikatu EUCC, na który ma to wpływ.

2. Na podstawie środków, o których mowa w ust. 1, jednostka certyfikująca przyjmuje jedną z następujących decyzji w odniesieniu do każdego certyfikatu EUCC, na który ma to wpływ:

a) utrzymuje certyfikat EUCC w niezmienionej postaci;

b) cofa certyfikat EUCC zgodnie z art. 14 lub art. 20 i, w stosownych przypadkach, wydaje nowy certyfikat EUCC.

3. Na podstawie środków, o których mowa w ust. 1, krajowy organ ds. certyfikacji cyberbezpieczeństwa:

a) w razie potrzeby zgłasza nieprzestrzeganie przepisów przez jednostkę certyfikującą lub powiązaną z nią ITSEF krajowej jednostce akredytującej;

b) w stosownych przypadkach ocenia potencjalny wpływ na zezwolenie.

ROZDZIAŁ VI

**ZARZĄDZANIE PODATNOŚCIAMI I UJAWNIANIE PODATNOŚCI**

*Artykuł 32*

**Zakres zarządzania podatnościami**

Niniejszy rozdział ma zastosowanie do produktów ICT, w odniesieniu do których wydano certyfikat EUCC.

SEKCJA I

## *ZARZĄDZANIE PODATNOŚCIAMI*

*Artykuł 33*

### Procedury zarządzania podatnościami

1. Posiadacz certyfikatu EUCC ustanawia i utrzymuje wszystkie niezbędne procedury zarządzania podatnościami zgodnie z zasadami określonymi w niniejszej sekcji oraz, w razie potrzeby, uzupełnione procedurami określonymi w normie EN ISO/IEC 30111.

2. Posiadacz certyfikatu EUCC utrzymuje i publikuje odpowiednie metody otrzymywania ze źródeł zewnętrznych, w tym od użytkowników, jednostek certyfikujących i ekspertów w obszarze bezpieczeństwa, informacji o podatnościach związanych z jego produktami.

3. W przypadku gdy posiadacz certyfikatu EUCC wykryje potencjalną podatność mającą wpływ na certyfikowany produkt ICT lub otrzyma informacje jej temat, rejestruje ją i przeprowadza analizę skutków podatności.

4. Jeżeli potencjalna podatność wpływa na produkt złożony, posiadacz certyfikatu EUCC informuje posiadacza zależnych certyfikatów EUCC o potencjalnej podatności.

5. Na uzasadniony wniosek jednostki certyfikującej, która wydała certyfikat, posiadacz certyfikatu EUCC przekazuje tej jednostce certyfikującej wszystkie istotne informacje na temat potencjalnych podatności.

*Artykuł 34*

### Analiza skutków podatności

1. Analiza skutków podatności musi odnosić się do celu oceny i oświadczeń o uzasadnieniu zaufania zawartych w certyfikacie Analizę skutków podatności przeprowadza się w terminie odpowiednim z punktu widzenia możliwości wykorzystania i krytyczności potencjalnej podatności certyfikowanego produktu ICT.

2. W stosownych przypadkach dokonuje się obliczenia potencjału ataku zgodnie z odpowiednią metodyką zawartą w normach, o których mowa w art. 3, oraz w odpowiednich dokumentach odzwierciedlających stan wiedzy wymienionych w załączniku I, aby ustalić możliwość wykorzystania podatności. Uwzględnia się poziom AVA_VAN certyfikatu EUCC.

*Artykuł 35*

### Sprawozdanie z analizy skutków podatności

1. Posiadacz sporządza sprawozdanie z analizy skutków podatności, jeżeli z analizy skutków wynika, że podatność ta ma prawdopodobny wpływ na zgodność produktu ICT z jego certyfikatem.

2. Sprawozdanie z analizy skutków podatności zawiera ocenę następujących elementów:

a) skutku podatności dla certyfikowanego produktu ICT;

b) możliwych zagrożeń związanych z bliskością lub dostępnością ataku;

c) tego, czy podatności można zaradzić;

d) w przypadku gdy podatności można zaradzić – możliwych sposobów usunięcia podatności.

3. Sprawozdanie z analizy skutków podatności zawiera, w stosownych przypadkach, szczegółowe informacje na temat możliwych sposobów wykorzystania podatności. Informacje dotyczące możliwych sposobów wykorzystania podatności są przetwarzane zgodnie z odpowiednimi środkami bezpieczeństwa, aby chronić ich poufność i zapewnić w razie potrzeby ich ograniczone rozpowszechnianie.

4. Posiadacz certyfikatu EUCC bez zbędnej zwłoki przekazuje sprawozdanie z analizy skutków podatności jednostce certyfikującej lub krajowemu organowi ds. certyfikacji cyberbezpieczeństwa zgodnie z art. 56 ust. 8 rozporządzenia (UE) 2019/881.

5. W przypadku gdy w sprawozdaniu z analizy skutków podatności stwierdzono, że podatność nie jest rezydualna w rozumieniu norm, o których mowa w art. 3, i że można jej zaradzić, zastosowanie ma art. 36.

6. W przypadku gdy w sprawozdaniu z analizy skutków podatności stwierdzono, że podatność nie jest rezydualna i że nie można jej zaradzić, certyfikat EUCC zostaje cofnięty zgodnie z art. 14.

7. Posiadacz certyfikatu EUCC monitoruje wszelkie rezydualne podatności w celu zapewnienia, aby nie można było ich wykorzystać w przypadku zmian w środowisku operacyjnym.

*Artykuł 36*

**Zaradzanie podatności**

Posiadacz certyfikatu EUCC przedkłada jednostce certyfikującej propozycję odpowiedniego działania zaradczego. Jednostka certyfikująca przeprowadza przegląd certyfikatu zgodnie z art. 13. Zakres tego przeglądu określa się na podstawie propozycji zaradzenia podatności.

*SEKCJA II*

***UJAWNIANIE PODATNOŚCI***

*Artykuł 37*

**Informacje udostępniane krajowemu organowi ds. certyfikacji cyberbezpieczeństwa**

1. Informacje przekazywane przez jednostkę certyfikującą krajowemu organowi ds. certyfikacji cyberbezpieczeństwa obejmują wszystkie elementy niezbędne krajowemu organowi ds. certyfikacji cyberbezpieczeństwa do zrozumienia skutków podatności, zmiany, jakie należy wprowadzić w produkcie ICT, oraz, o ile są dostępne, wszelkie informacje jednostki certyfikującej na temat szerszych konsekwencji podatności dla innych certyfikowanych produktów ICT.

2. Informacje przekazywane zgodnie z ust. 1 nie mogą zawierać szczegółowych informacji na temat sposobów wykorzystania podatności. Przepis ten pozostaje bez uszczerbku dla uprawnień dochodzeniowych krajowego organu ds. certyfikacji cyberbezpieczeństwa.

*Artykuł 38*

**Współpraca z innymi krajowymi organami ds. certyfikacji cyberbezpieczeństwa**

1. Krajowy organ ds. certyfikacji cyberbezpieczeństwa udostępnia odpowiednie informacje otrzymane zgodnie z art. 37 innym krajowym organom ds. certyfikacji cyberbezpieczeństwa i ENISA.

2. Inne krajowe organy ds. certyfikacji cyberbezpieczeństwa mogą podjąć decyzję o dalszej analizie podatności lub, po poinformowaniu posiadacza certyfikatu EUCC, zwrócić się do odpowiednich jednostek certyfikujących o ocenę, czy podatność może mieć wpływ na inne certyfikowane produkty ICT.

*Artykuł 39*

**Podawanie do wiadomości publicznej informacji o podatności**

Po cofnięciu certyfikatu posiadacz certyfikatu EUCC ujawnia i rejestruje wszelkie publicznie znane i wyeliminowane podatności w produkcie ICT w europejskiej bazie danych dotyczących podatności, utworzonej zgodnie z art. 12 dyrektywy Parla-

mentu Europejskiego i Rady (UE) 2022/2555 ([5]), lub w innych repozytoriach internetowych, o których mowa w art. 55 ust. 1 lit. d) rozporządzenia (UE) 2019/881.

ROZDZIAŁ VII

**PRZECHOWYWANIE, UJAWNIANIE I OCHRONA INFORMACJI**

*Artykuł 40*

**Przechowywanie dokumentów przez jednostki certyfikujące i ITSEF**

1. ITSEF i jednostki certyfikujące prowadzą system dokumentacji, który zawiera wszystkie dokumenty sporządzone w związku z każdą przeprowadzoną przez nie oceną i certyfikacją.

2. Jednostki certyfikujące i ITSEF przechowują dokumentację w bezpieczny sposób i przez okres niezbędny do celów niniejszego rozporządzenia oraz przez co najmniej 5 lat po cofnięciu odpowiedniego certyfikatu EUCC. Gdy jednostka certyfikująca wydaje nowy certyfikat EUCC zgodnie z art. 13 ust. 2 lit. c), przechowuje dokumentację cofniętego certyfikatu EUCC wraz z nowym certyfikatem EUCC i tak długo jak w przypadku nowego certyfikatu EUCC.

*Artykuł 41*

**Informacje udostępniane przez posiadacza certyfikatu**

1. Informacje, o których mowa w art. 55 rozporządzenia (UE) 2019/881, muszą być dostępne w języku łatwo zrozumiałym dla użytkowników.

2. Posiadacz certyfikatu EUCC przechowuje w bezpieczny sposób przez okres niezbędny do celów niniejszego rozporządzenia i przez co najmniej 5 lat po cofnięciu odpowiedniego certyfikatu EUCC:

a) dokumentację informacji przekazanych jednostce certyfikującej i ITSEF w trakcie procesu certyfikacji;

b) egzemplarz certyfikowanego produktu ICT.

3. Gdy jednostka certyfikująca wydaje nowy certyfikat EUCC zgodnie z art. 13 ust. 2 lit. c), posiadacz przechowuje dokumentację cofniętego certyfikatu EUCC wraz z nowym certyfikatem EUCC i tak długo jak w przypadku nowego certyfikatu EUCC.

4. Na wniosek jednostki certyfikującej lub krajowego organu ds. certyfikacji cyberbezpieczeństwa posiadacz certyfikatu EUCC udostępnia dokumentację i kopie, o których mowa w ust. 2.

*Artykuł 42*

**Informacje udostępniane przez ENISA**

1. ENISA publikuje na stronie internetowej, o której mowa w art. 50 ust. 1 rozporządzenia (UE) 2019/881, następujące informacje:

a) wszystkie certyfikaty EUCC;

b) informacje o statusie certyfikatu EUCC, w szczególności o tym, czy certyfikat ten jest w mocy, został zawieszony, został cofnięty lub wygasł;

c) sprawozdania z certyfikacji odpowiadające każdemu certyfikatowi EUCC;

([5]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

d) wykaz akredytowanych jednostek oceniających zgodność;

e) wykaz jednostek oceniających zgodność posiadających zezwolenie;

f) dokumenty odzwierciedlające stan wiedzy wymienione w załączniku I;

g) opinie Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa, o których mowa w art. 62 ust. 4 lit. c) rozporządzenia (UE) 2019/881;

h) sprawozdania z wzajemnej oceny wydane zgodnie z art. 47.

2. Informacje, o których mowa w ust. 1, udostępnia się co najmniej w języku angielskim.

3. Jednostki certyfikujące oraz, w stosownych przypadkach, krajowe organy ds. certyfikacji cyberbezpieczeństwa niezwłocznie informują ENISA o swoich decyzjach mających wpływ na treść lub status certyfikatu EUCC, o którym to statusie mowa w ust. 1 lit. b).

4. ENISA zapewnia, aby w informacjach publikowanych zgodnie z ust. 1 lit. a), b) i c) jasno wskazywano wersje certyfikowanego produktu ICT, które są objęte certyfikatem EUCC.

*Artykuł 43*

**Ochrona informacji**

Jednostki oceniające zgodność, krajowe organy ds. certyfikacji cyberbezpieczeństwa, ECCG, ENISA, Komisja i wszystkie inne strony zapewniają bezpieczeństwo i ochronę tajemnic handlowych i innych informacji poufnych, w tym tajemnic przedsiębiorstwa, a także ochronę praw własności intelektualnej, oraz wprowadzają niezbędne i odpowiednie środki techniczne i organizacyjne.

ROZDZIAŁ VIII

**UMOWY O WZAJEMNYM UZNAWANIU Z PAŃSTWAMI TRZECIMI**

*Artykuł 44*

**Warunki**

1. Państwa trzecie, które chcą certyfikować swoje produkty zgodnie z niniejszym rozporządzeniem i które chcą, aby taka certyfikacja była uznawana w Unii, zawierają z Unią umowę o wzajemnym uznawaniu.

2. Umowa o wzajemnym uznawaniu obejmuje mające zastosowanie poziomy uzasadnienia zaufania w odniesieniu do certyfikowanych produktów ICT oraz, w stosownych przypadkach, profili zabezpieczeń.

3. Umowy o wzajemnym uznawaniu, o których mowa w ust. 1, można zawierać wyłącznie z państwami trzecimi, które spełniają następujące warunki:

a) mają organ, który:

   1) jest podmiotem publicznym, niezależnym od podmiotów, które nadzoruje i monitoruje, pod względem struktury organizacyjnej i prawnej, finansowania i podejmowania decyzji;

   2) dysponuje odpowiednimi uprawnieniami w zakresie monitorowania i nadzoru w celu prowadzenia dochodzeń oraz jest uprawniony do wprowadzania odpowiednich środków naprawczych w celu zapewnienia zgodności;

   3) ma system skutecznych, proporcjonalnych i odstraszających kar w celu zapewnienia zgodności;

   4) zgadza się na współpracę z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa i ENISA w celu wymiany najlepszych praktyk i informacji na temat odpowiednich zmian w dziedzinie certyfikacji cyberbezpieczeństwa oraz na działanie na rzecz jednolitej interpretacji obecnie mających zastosowanie kryteriów i metod oceny, między innymi przez stosowanie zharmonizowanej dokumentacji równoważnej dokumentom odzwierciedlającym stan wiedzy wymienionym w załączniku I;

b) mają niezależną jednostkę akredytującą przeprowadzającą akredytacje przy użyciu norm równoważnych normom, o których mowa w rozporządzeniu (WE) nr 765/2008;

c) zobowiązują się, że procesy i procedury oceny i certyfikacji będą przeprowadzane w sposób należycie profesjonalny, z uwzględnieniem zgodności z normami międzynarodowymi, o których mowa w niniejszym rozporządzeniu, w szczególności w art. 3;

d) mają zdolność do zgłaszania wcześniej niewykrytych podatności oraz ustanowioną odpowiednią procedurę zarządzania podatnościami i ujawniania podatności;

e) ustanowiły procedury umożliwiające im skuteczne składanie i rozpatrywanie skarg oraz zapewnienie skarżącemu skutecznego środka ochrony prawnej;

f) ustanowiły mechanizm współpracy z innymi organami Unii i państw członkowskich istotnymi dla certyfikacji cyberbezpieczeństwa na podstawie niniejszego rozporządzenia, w tym w zakresie wymiany informacji na temat ewentualnej niezgodności certyfikatów, monitorowania odpowiednich zmian w dziedzinie certyfikacji oraz zapewnienia wspólnego podejścia do utrzymywania i przeglądu certyfikacji.

4. Oprócz warunków określonych w ust. 3 umowę o wzajemnym uznawaniu, o której mowa w ust. 1, obejmującą poziom uzasadnienia zaufania „wysoki" można zawrzeć z państwami trzecimi tylko wtedy, gdy spełnione są również następujące warunki:

a) państwo trzecie ma niezależny i publiczny organ ds. certyfikacji cyberbezpieczeństwa, który prowadzi lub deleguje działania w zakresie oceny niezbędne do umożliwienia certyfikacji na poziomie uzasadnienia zaufania „wysoki" równoważne wymogom i procedurom określonym dla krajowych organów ds. cyberbezpieczeństwa w niniejszym rozporządzeniu i w rozporządzeniu (UE) 2019/881;

b) umowa o wzajemnym uznawaniu ustanawia wspólny mechanizm równoważny wzajemnej ocenie na potrzeby certyfikacji EUCC, aby usprawnić wymianę praktyk i wspólnie rozwiązywać problemy w dziedzinie oceny i certyfikacji.

ROZDZIAŁ IX

## WZAJEMNA OCENA JEDNOSTEK CERTYFIKUJĄCYCH

*Artykuł 45*

### Procedura wzajemnej oceny

1. Jednostkę certyfikującą wydającą certyfikaty EUCC o poziomie uzasadnienia zaufania „wysoki" poddaje się wzajemnej ocenie regularnie i co najmniej co 5 lat. Poszczególne typy wzajemnej oceny są wymienione w załączniku VI.

2. Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa sporządza i utrzymuje harmonogram wzajemnych ocen, zapewniając przestrzeganie takiej częstotliwości. Z wyjątkiem należycie uzasadnionych przypadków wzajemne oceny przeprowadza się na miejscu.

3. Wzajemna ocena może opierać się na dowodach zgromadzonych w trakcie poprzednich wzajemnych ocen lub równoważnych procedur jednostki certyfikującej poddanej wzajemnej ocenie lub krajowego organu ds. certyfikacji cyberbezpieczeństwa, pod warunkiem że:

a) wyniki nie są starsze niż 5 lat;

b) wynikom towarzyszy opis procedur wzajemnej oceny ustanowionych dla tego programu, jeżeli odnoszą się one do wzajemnej oceny przeprowadzonej w ramach innego programu certyfikacji;

c) w sprawozdaniu z wzajemnej oceny, o którym mowa w art. 47, określa się, które wyniki zostały ponownie wykorzystane z dalszą oceną lub bez takiej oceny.

4. W przypadku gdy wzajemna ocena obejmuje domenę techniczną, ocenia się również zainteresowaną ITSEF.

5. Jednostka certyfikująca poddana wzajemnej ocenie oraz, w razie potrzeby, krajowy organ ds. certyfikacji cyberbezpieczeństwa zapewniają, aby wszystkie istotne informacje były udostępniane zespołowi ds. wzajemnej oceny.

6. Wzajemną ocenę przeprowadza zespół ds. wzajemnej oceny utworzony zgodnie z załącznikiem VI.

*Artykuł 46*

**Etapy wzajemnej oceny**

1. Na etapie przygotowawczym członkowie zespołu ds. wzajemnej oceny dokonują przeglądu dokumentacji jednostki certyfikującej, obejmującej jej polityki i procedury, w tym wykorzystanie dokumentów odzwierciedlających stan wiedzy.

2. Na etapie wizyty na miejscu zespół ds. wzajemnej oceny ocenia kompetencje techniczne jednostki oraz, w stosownych przypadkach, kompetencje ITSEF, która przeprowadziła co najmniej jedną ocenę produktu ICT objętą wzajemną oceną.

3. Czas trwania etapu wizyty na miejscu może zostać przedłużony lub skrócony w zależności od takich czynników, jak możliwość ponownego wykorzystania istniejących dowodów i wyników z wzajemnej oceny lub liczba ITSEF i domen technicznych, w odniesieniu do których jednostka certyfikująca wydaje certyfikaty.

4. W stosownych przypadkach zespół ds. wzajemnej oceny określa kompetencje techniczne każdej ITSEF, odwiedzając jej laboratorium lub laboratoria techniczne oraz przeprowadzając wywiady z jej oceniającymi w odniesieniu do danej domeny technicznej i powiązanych konkretnych metod ataku.

5. Na etapie opracowywania sprawozdania zespół ds. oceny dokumentuje poczynione ustalenia w sprawozdaniu z wzajemnej oceny wraz z opinią oraz, w stosownych przypadkach, wykazem zaobserwowanych niezgodności, z których każdą klasyfikuje się według poziomu krytyczności.

6. Sprawozdanie z wzajemnej oceny musi najpierw zostać omówione z jednostką certyfikującą poddaną wzajemnej ocenie. Następnie, po omówieniu sprawozdania, jednostka certyfikująca ustala harmonogram środków, które należy wprowadzić w celu zastosowania się do ustaleń.

*Artykuł 47*

**Sprawozdanie z wzajemnej oceny**

1. Zespół ds. wzajemnej oceny przekazuje jednostce certyfikującej poddanej wzajemnej ocenie projekt sprawozdania z wzajemnej oceny.

2. Jednostka certyfikująca poddana wzajemnej ocenie przedkłada zespołowi ds. wzajemnej oceny uwagi dotyczące ustaleń oraz wykaz zobowiązań mających na celu wyeliminowanie niedociągnięć wskazanych w projekcie sprawozdania z wzajemnej oceny.

3. Zespół ds. wzajemnej oceny przedkłada Europejskiej Grupie ds. Certyfikacji Cyberbezpieczeństwa końcowe sprawozdanie z wzajemnej oceny, które zawiera również uwagi i zobowiązania jednostki certyfikującej poddanej wzajemnej ocenie. Zespół ds. wzajemnej oceny przedstawia również swoje stanowisko w sprawie uwag oraz tego, czy zobowiązania te wystarczają do wyeliminowania stwierdzonych niedociągnięć.

4. W przypadku stwierdzenia niezgodności w sprawozdaniu z wzajemnej oceny Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa może wyznaczyć jednostce certyfikującej poddanej wzajemnej ocenie odpowiedni termin na wyeliminowanie niezgodności.

5. Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa przyjmuje opinię w sprawie sprawozdania z wzajemnej oceny:

a) w przypadku gdy w sprawozdaniu z wzajemnej oceny nie stwierdza się niezgodności lub gdy jednostka certyfikująca poddana wzajemnej ocenie odpowiednio wyeliminowała niezgodności, Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa może wydać opinię pozytywną, a wszystkie odpowiednie dokumenty publikuje się na stronie internetowej ENISA poświęconej certyfikacji;

b) w przypadku gdy jednostka certyfikująca poddana wzajemnej ocenie nie wyeliminuje niezgodności w odpowiedni sposób w wyznaczonym terminie, Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa może wydać opinię negatywną, którą publikuje się na stronie internetowej ENISA poświęconej certyfikacji, wraz ze sprawozdaniem z wzajemnej oceny i wszystkimi odpowiednimi dokumentami.

6. Przed opublikowaniem opinii z publikowanych dokumentów usuwa się wszelkie informacje szczególnie chronione, dane osobowe lub informacje zastrzeżone.

ROZDZIAŁ X

**UTRZYMANIE PROGRAMU**

*Artykuł 48*

**Utrzymanie EUCC**

1. Komisja może zwrócić się do Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa o przyjęcie opinii w świetle utrzymania EUCC i podjęcie niezbędnych prac przygotowawczych.

2. Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa może przyjąć opinię w celu zatwierdzenia dokumentów odzwierciedlających stan wiedzy.

3. ENISA publikuje dokumenty odzwierciedlające stan wiedzy, które zatwierdziła Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa.

ROZDZIAŁ XI

**PRZEPISY KOŃCOWE**

*Artykuł 49*

**Programy krajowe objęte EUCC**

1. Zgodnie z art. 57 ust. 1 rozporządzenia (UE) 2019/881 i bez uszczerbku dla art. 57 ust. 3 tego rozporządzenia wszystkie krajowe programy certyfikacji cyberbezpieczeństwa i powiązane z nimi procedury dotyczące produktów ICT i procesów ICT, które są objęte EUCC, przestają być skuteczne po upływie 12 miesięcy od wejścia w życie niniejszego rozporządzenia.

2. Na zasadzie odstępstwa od art. 50 proces certyfikacji może zostać zainicjowany w ramach krajowego programu certyfikacji cyberbezpieczeństwa w okresie 12 miesięcy od wejścia w życie niniejszego rozporządzenia, pod warunkiem, że ten proces certyfikacji zostanie zakończony nie później niż 24 miesiące po wejściu w życie niniejszego rozporządzenia.

3. Certyfikaty wydane w ramach krajowych programów certyfikacji cyberbezpieczeństwa mogą podlegać przeglądowi. Nowe certyfikaty zastępujące zweryfikowane certyfikaty wydaje się zgodnie z niniejszym rozporządzeniem.

*Artykuł 50*

**Wejście w życie**

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

Niniejsze rozporządzenie stosuje się od dnia 27 lutego 2025 r.

Rozdział IV i załącznik V stosuje się od dnia wejścia w życie niniejszego rozporządzenia.

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

Sporządzono w Brukseli dnia 31 stycznia 2024 r.

*W imieniu Komisji*
*Przewodnicząca*
Ursula VON DER LEYEN

*ZAŁĄCZNIK I*

**Domeny techniczne i dokumenty odzwierciedlające stan wiedzy**

1. Domeny techniczne na poziomach AVA_VAN 4 lub 5:

   a) dokumenty powiązane ze zharmonizowaną oceną domeny technicznej „Karty elektroniczne i podobne urządzenia", a w szczególności następujące dokumenty w wersjach obowiązujących dnia [data wejścia w życie] r.:

      1) „Minimum ITSEF requirements for security evaluations of smart cards and similar devices" [„Minimalne wymogi ITSEF dotyczące oceny bezpieczeństwa kart elektronicznych i podobnych urządzeń"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

      2) „Minimum Site Security Requirements" [„Minimalne wymogi bezpieczeństwa strony"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

      3) „Application of Common Criteria to integrated circuits" [„Stosowanie wspólnych kryteriów do układów scalonych"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

      4) „Security Architecture requirements (ADV_ARC) for smart cards and similar devices" [„Wymogi architektury bezpieczeństwa (ADV_ARC) dotyczące kart elektronicznych i podobnych urządzeń"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

      5) „Certification of »open« smart card products" [„Certyfikacja »otwartych« produktów kart elektronicznych"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

      6) „Composite product evaluation for smart cards and similar devices" [„Ocena produktu złożonego w przypadku kart elektronicznych i podobnych urządzeń"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

      7) „Application of Attack Potential to Smartcards" [„Zastosowanie potencjału ataku do kart elektronicznych"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

   b) dokumenty powiązane ze zharmonizowaną oceną domeny technicznej „Urządzenia sprzętowe ze skrzynkami bezpieczeństwa", a w szczególności następujące dokumenty w wersjach obowiązujących dnia [data wejścia w życie] r.:

      1) „Minimum ITSEF requirements for security evaluations of hardware devices with security boxes" [„Minimalne wymogi ITSEF dotyczące ocen bezpieczeństwa urządzeń sprzętowych ze skrzynkami bezpieczeństwa"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

      2) „Minimum Site Security Requirements" [„Minimalne wymogi bezpieczeństwa strony"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.;

      3) „Application of Attack Potential to hardware devices with security boxes" [„Zastosowanie potencjału ataku do urządzeń sprzętowych ze skrzynkami bezpieczeństwa"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r.

2. Dokumenty odzwierciedlające stan wiedzy w wersjach obowiązujących dnia [data wejścia w życie] r.:

   a) dokumenty powiązane ze zharmonizowaną akredytacją jednostek oceniających zgodność: „Accreditation of ITSEFs for the EUCC" [„Akredytacja ITSEF na potrzeby EUCC"], wstępnie zatwierdzony przez ECCG dnia 20 października 2023 r..

*ZAŁĄCZNIK II*

**Profile zabezpieczeń certyfikowane na poziomie AVA_VAN 4 lub 5**

1. W przypadku kategorii kwalifikowanych urządzeń do składania podpisu i pieczęci na odległość:

1) EN 419241-2:2019 – Wiarygodne systemy serwerów obsługujących podpisy – Część 2: Profil zabezpieczeń dla QSCD dla serwerów obsługujących podpisy;

2) EN 419221-5: 2018 – Profile zabezpieczeń dla modułów kryptograficznych TSP – Część 5: moduł kryptograficzny dla usług zaufania;

2. Profile zabezpieczeń, które przyjęto jako dokumenty odzwierciedlające stan wiedzy:

[BRAK]

*ZAŁĄCZNIK III*

**Zalecane profile zabezpieczeń (ilustrujące domeny techniczne z załącznika I)**

Profile zabezpieczeń stosowane w certyfikacji produktów ICT należących do niżej wymienionych kategorii produktów ICT:

a) w przypadku kategorii dokumentów podróży odczytywanych maszynowo:

1) profil zabezpieczeń dokumentu podróży odczytywanego maszynowo z wykorzystaniem standardowej procedury inspekcji z protokołem PACE, BSI-CC-PP-0068-V2-2011-MA-01;

2) profil zabezpieczeń dokumentu podróży odczytywanego maszynowo z rozszerzoną kontrolą dostępu „aplikacji ICAO", BSI-CC-PP-0056-2009;

3) profil zabezpieczeń dokumentu podróży odczytywanego maszynowo z rozszerzoną kontrolą dostępu „aplikacji ICAO" z protokołem PACE, BSI-CC-PP-0056-V2-2012-MA-02;

4) profil zabezpieczeń dokumentu podróży odczytywanego maszynowo z podstawową kontrolą dostępu „aplikacji ICAO", BSI-CC-PP-0055-2009;

b) w przypadku kategorii urządzeń do składania podpisu elektronicznego:

1) EN 419211-1: 2014 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 1: Przegląd

2) EN 419211-2:2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 2: Urządzenie z generowaniem kluczy;

3) EN 419211-3:2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 3: Urządzenie z importem kluczy;

4) EN 419211-4:2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 4: Rozszerzenie dla urządzenia z generowaniem kluczy i zaufanym kanałem z aplikacją generującą certyfikaty

5) EN 419211-5:2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 5: Rozszerzenie dla urządzenia z generowaniem kluczy i zaufanym kanałem z aplikacją do składania podpisu;

6) EN 419211-6:2014 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 6: Rozszerzenie dla urządzenia z importem kluczy i zaufanym kanałem z aplikacją do składania podpisu;

c) w przypadku kategorii tachografów cyfrowych:

1) tachograf cyfrowy – karta do tachografu, o której mowa w rozporządzeniu wykonawczym Komisji (UE) 2016/799 z dnia 18 marca 2016 r. w sprawie wykonania rozporządzenia (UE) nr 165/2014 (załącznik I C);

2) tachograf cyfrowy – przyrząd rejestrujący, o którym mowa w załączniku I B do rozporządzenia Komisji (WE) nr 1360/2002, przeznaczony do instalowania w pojazdach transportu drogowego;

3) tachograf cyfrowy – urządzenie zewnętrzne GNSS (profil zabezpieczeń EGF), o którym mowa w załączniku I C do rozporządzenia wykonawczego Komisji (UE) 2016/799 z dnia 18 marca 2016 r. w sprawie wykonania rozporządzenia (UE) Parlamentu Europejskiego i Rady nr 165/2014;

4) tachograf cyfrowy – czujnik ruchu (profil zabezpieczeń czujnika ruchu), o którym mowa w załączniku I C do rozporządzenia wykonawczego Komisji (UE) 2016/799 z dnia 18 marca 2016 r. w sprawie wykonania rozporządzenia (UE) Parlamentu Europejskiego i Rady nr 165/2014;

d) w przypadku kategorii układów scalonych, kart elektronicznych i powiązanych urządzeń:

1) profil zabezpieczeń platformy bezpieczeństwa układów scalonych, BSI-CC-PP-0084-2014;

2) Java Card System – otwarta konfiguracja, V3.0.5 BSI-CC-PP-0099-2017;

3) Java Card System – zamknięta konfiguracja, BSI-CC-PP-0101-2017;

4) profil zabezpieczeń dla modułu zaufanej platformy dla komputerów PC rodziny 2.0, poziom 0, wersja 1.16, ANSSI-CC-PP-2015/07;

5) uniwersalna karta SIM, PU-2009-RT-79, ANSSI-CC-PP-2010/04;

6) wbudowana uniwersalna karta z układem scalonym (eUICC) do urządzeń komunikacji maszyna–maszyna, BSI-CC-PP-0089-2015;

e) w przypadku kategorii punktów interakcji (płatności) i terminali płatniczych:

1) punkt interakcji „POI-CHIP-ONLY", ANSSI-CC-PP-2015/01;

2) punkt interakcji „POI-CHIP-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/02;

3) punkt interakcji „POI-COMPREHENSIVE", ANSSI-CC-PP-2015/03;

4) punkt interakcji „POI-COMPREHENSIVE and Open Protocol Package", ANSSI-CC-PP-2015/04;

5) punkt interakcji „POI-PED-ONLY", ANSSI-CC-PP-2015/05;

6) punkt interakcji „POI-PED-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/06;

f) w przypadku kategorii urządzeń sprzętowych ze skrzynkami bezpieczeństwa:

1) moduł kryptograficzny dla dostawcy kryptograficznych usług operacji podpisu z kopią zapasową – PP CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

2) moduł kryptograficzny dla dostawcy kryptograficznych usług generowania klucza – PP CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

3) moduł kryptograficzny dla dostawcy kryptograficznych usług operacji podpisu bez kopii zapasowej – PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

*ZAŁĄCZNIK IV*

## Ciągłość uzasadnienia zaufania i przegląd certyfikatów

### IV.1 Ciągłość uzasadnienia zaufania: zakres

1. Następujące wymogi dotyczące uzasadnienia zaufania mają zastosowanie do działań w zakresie utrzymania związanych z:

   a) ponowną oceną, czy niezmieniony certyfikowany produkt ICT nadal spełnia wymogi bezpieczeństwa,

   b) oceną skutków zmian w certyfikowanym produkcie ICT dla jego certyfikacji;

   c) jeżeli uwzględniono w certyfikacie – stosowaniem poprawek zgodnie z ocenionym procesem zarządzania poprawkami;

   d) jeżeli uwzględniono – przeglądem procesów zarządzania cyklem życia lub produkcji posiadacza certyfikatu.

2. Posiadacz certyfikatu EUCC może wystąpić o przegląd certyfikatu w następujących przypadkach:

   a) certyfikat EUCC wygaśnie w ciągu dziewięciu miesięcy;

   b) w certyfikowanym produkcie ICT albo w innym czynniku nastąpiła zmiana, która może mieć wpływ na jego funkcje bezpieczeństwa;

   c) posiadacz certyfikatu domaga się ponownego przeprowadzenia oceny podatności w celu ponownego potwierdzenia uzasadnienia zaufania certyfikatu EUCC związanego z odpornością produktu ICT na obecne cyberataki.

### IV.2 Ponowna ocena

1. W przypadku gdy zachodzi potrzeba oceny skutków zmian w środowisku zagrożeń niezmienionego certyfikowanego produktu ICT, jednostce certyfikującej przedkłada się wniosek o ponowną ocenę.

2. Ponowną ocenę przeprowadza ta sama ITSEF, która była zaangażowana w poprzednią ocenę, z ponownym wykorzystaniem wszystkich jej wyników, które nadal mają zastosowanie. Ocena skupia się na działaniach w zakresie uzasadnienia zaufania, na które może mieć wpływ zmienione środowisko zagrożeń certyfikowanego produktu ICT, w szczególności na odpowiedniej rodzinie AVA_VAN, a ponadto na rodzinie cyklu życia uzasadnienia zaufania (ALC), w ramach której ponownie gromadzi się wystarczające dowody na utrzymanie środowiska rozwojowego.

3. ITSEF opisuje zmiany i szczegółowo przedstawia wyniki ponownej oceny wraz z aktualizacją poprzedniego sprawozdania technicznego z oceny.

4. Jednostka certyfikująca dokonuje przeglądu zaktualizowanego sprawozdania technicznego z oceny i sporządza sprawozdanie z ponownej oceny. Status pierwotnego certyfikatu zostaje następnie zmieniony zgodnie z art. 13.

5. Sprawozdanie z ponownej oceny i zaktualizowany certyfikat przekazuje się krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i ENISA do publikacji na jej stronie internetowej poświęconej certyfikacji cyberbezpieczeństwa.

### IV.3 Zmiany w certyfikowanym produkcie ICT

1. W przypadku gdy certyfikowany produkt ICT został zmieniony, posiadacz certyfikatu, który chce utrzymać certyfikat, przedkłada jednostce certyfikującej sprawozdanie z analizy skutków.

2. Sprawozdanie z analizy skutków zawiera następujące elementy:

   a) wprowadzenie zawierające informacje niezbędne do wskazania sprawozdania z analizy skutków oraz celu oceny podlegającego zmianom;

b) opis zmian w produkcie;

c) wskazanie dowodów twórcy, na które zmiany mają wpływ;

d) opis modyfikacji dowodów twórcy;

e) ustalenia i wnioski dotyczące skutków każdej zmiany dla uzasadnienia zaufania.

3. Jednostka certyfikująca bada zmiany opisane w sprawozdaniu z analizy skutków w celu potwierdzenia ich skutków dla uzasadnienia zaufania w odniesieniu do certyfikowanego celu oceny, jak zaproponowano we wnioskach ze sprawozdania z analizy skutków.

4. Po przeprowadzeniu badania jednostka certyfikująca określa skalę zmiany jako nieistotną lub istotną w zależności od jej skutków.

5. W przypadku gdy jednostka certyfikująca potwierdziła, że zmiany są nieistotne, wydaje się nowy certyfikat dla zmienionego produktu ICT oraz sporządza się sprawozdanie z utrzymania dotyczące pierwotnego sprawozdania z certyfikacji, na następujących warunkach:

a) sprawozdanie z utrzymania ujmuje się jako podzbiór sprawozdania z analizy skutków, zawierający następujące sekcje:

1) wprowadzenie;

2) opis zmian;

3) dowody twórcy, na które zmiany mają wpływ;

b) data ważności nowego certyfikatu nie może przekraczać daty pierwotnego certyfikatu.

6. Nowy certyfikat zawierający sprawozdanie z utrzymania przekazuje się ENISA do publikacji na jej stronie internetowej poświęconej certyfikacji cyberbezpieczeństwa.

7. W przypadku potwierdzenia, że zmiany są istotne, przeprowadza się ponowną ocenę w kontekście poprzedniej oceny i z ponownym wykorzystaniem wszelkich wyników poprzedniej oceny, które nadal mają zastosowanie.

8. Po zakończeniu oceny zmienionego celu oceny ITSEF sporządza nowe sprawozdanie techniczne z oceny. Jednostka certyfikująca dokonuje przeglądu zaktualizowanego sprawozdania technicznego z oceny i, w stosownych przypadkach, wydaje nowy certyfikat wraz z nowym sprawozdaniem z certyfikacji.

9. Nowy certyfikat i sprawozdanie z certyfikacji przekazuje się ENISA do publikacji.

### IV.4 **Zarządzanie poprawkami**

1. Procedura zarządzania poprawkami przewiduje ustrukturyzowany proces aktualizacji certyfikowanego produktu ICT. Procedurę zarządzania poprawkami, w tym mechanizm wprowadzony w produkcie ICT przez wnioskodawcę ubiegającego się o certyfikację, można stosować po certyfikacji produktu ICT na odpowiedzialność jednostki oceniającej zgodność.

2. Wnioskodawca ubiegający się o certyfikację może włączyć do certyfikacji produktu ICT mechanizm poprawek jako część certyfikowanej procedury zarządzania wprowadzonej w produkcie ICT pod jednym z następujących warunków:

a) funkcje, na które poprawka ma wpływ, znajdują się poza celem oceny certyfikowanego produktu ICT;

b) poprawka odnosi się do wcześniej określonej nieistotnej zmiany certyfikowanego produktu ICT;

c) poprawka dotyczy potwierdzonej podatności mającej krytyczny wpływ na bezpieczeństwo certyfikowanego produktu ICT.

3. Jeżeli poprawka dotyczy istotnej zmiany celu oceny certyfikowanego produktu ICT w odniesieniu do wcześniej niewykrytej podatności, która nie ma krytycznego wpływu na bezpieczeństwo produktu ICT, zastosowanie mają przepisy art. 13.

4. Procedura zarządzania poprawkami do produktu ICT będzie składała się z następujących elementów:

   a) procesu opracowania i publikacji poprawek dla produktu ICT;

   b) mechanizmu technicznego i funkcji służących do wprowadzenia poprawek do produktu ICT;

   c) zestawu działań w zakresie oceny związanych ze skutecznością i działaniem mechanizmu technicznego.

5. Podczas certyfikacji produktu ICT:

   a) wnioskodawca ubiegający się o certyfikację produktu ICT przedstawia opis procedury zarządzania poprawkami;

   b) ITSEF weryfikuje następujące elementy:

      1) czy twórca wdrożył mechanizmy poprawek w produkcie ICT zgodnie z procedurą zarządzania poprawkami, którą przedłożono do certyfikacji;

      2) czy granice celu oceny są rozdzielone w taki sposób, by zmiany wprowadzone w rozdzielonych procesach nie miały wpływu na bezpieczeństwo celu oceny;

      3) czy techniczny mechanizm poprawek działa zgodnie z przepisami niniejszej sekcji i twierdzeniami wnioskodawcy;

   c) jednostka certyfikująca uwzględnia w sprawozdaniu z certyfikacji wynik ocenionej procedury zarządzania poprawkami.

6. Posiadacz certyfikatu może przystąpić do stosowania opracowanej poprawki zgodnie z certyfikowaną procedurą zarządzania poprawkami do danego certyfikowanego produktu ICT i w ciągu pięciu dni roboczych podejmuje następujące kroki w następujących przypadkach:

   a) w przypadku, o którym mowa w pkt 2 lit. a), zgłasza daną poprawkę jednostce certyfikującej, która nie zmienia odpowiedniego certyfikatu EUCC;

   b) w przypadku, o którym mowa w pkt 2 lit. b), przedkłada daną poprawkę ITSEF do przeglądu. ITSEF informuje jednostkę certyfikującą po otrzymaniu poprawki, po czym jednostka certyfikująca podejmuje odpowiednie działanie w celu wydania nowej wersji odpowiedniego certyfikatu EUCC i aktualizacji sprawozdania z certyfikacji;

   c) w przypadku, o którym mowa w pkt 2 lit. c), przedkłada daną poprawkę ITSEF w celu dokonania koniecznej ponownej oceny, ale równolegle może udostępnić poprawkę. ITSEF informuje o tym jednostkę certyfikującą, po czym jednostka certyfikująca rozpoczyna powiązane działania związane z certyfikacją.

*ZAŁĄCZNIK V*

**Treść sprawozdania z certyfikacji**

## V.1 **Sprawozdanie z certyfikacji**

1. Na podstawie sprawozdań technicznych z oceny przedstawionych przez ITSEF jednostka certyfikująca sporządza sprawozdanie z certyfikacji, które ma być opublikowane wraz z odpowiednim certyfikatem EUCC.

2. Sprawozdanie z certyfikacji jest źródłem szczegółowych i praktycznych informacji na temat produktu ICT lub kategorii produktów ICT oraz na temat bezpiecznego wdrożenia produktu ICT, a zatem musi zawierać wszystkie publicznie dostępne i możliwe do udostępnienia informacje istotne dla użytkowników i zainteresowanych stron. W sprawozdaniu z certyfikacji można przywoływać publicznie dostępne i możliwe do udostępnienia informacje.

3. Sprawozdanie z certyfikacji zawiera co najmniej następujące sekcje:

   a) streszczenie;

   b) identyfikację produktu ICT lub kategorii produktów ICT w odniesieniu do profili zabezpieczeń;

   c) usługi w zakresie bezpieczeństwa;

   d) założenia i sprecyzowanie zakresu;

   e) informacje dotyczące architektury;

   f) w stosownych przypadkach – dodatkowe informacje na temat cyberbezpieczeństwa;

   g) badanie produktów ICT, jeżeli zostało przeprowadzone;

   h) w stosownych przypadkach – dane identyfikacyjne procesów zarządzania cyklem życia oraz obiektów produkcyjnych posiadacza certyfikatu;

   i) wyniki oceny i informacje dotyczące certyfikatu;

   j) podsumowanie celu bezpieczeństwa produktu ICT przedłożonego do certyfikacji;

   k) znak lub etykietę związane z programem, o ile są dostępne;

   l) bibliografię.

4. Streszczenie jest krótkim streszczeniem całego sprawozdania z certyfikacji. Streszczenie zawiera jasny i zwięzły przegląd wyników oceny oraz następujące informacje:

   a) nazwę ocenionego produktu ICT, wyliczenie komponentów produktu stanowiących część oceny, oraz wersję produktu ICT;

   b) nazwę ITSEF, która przeprowadziła ocenę, oraz, w stosownych przypadkach, wykaz podwykonawców;

   c) datę zakończenia oceny;

   d) odniesienie do sprawozdania technicznego z oceny sporządzonego przez ITSEF;

   e) krótki opis wyników sprawozdania z certyfikacji, w tym:

      1) wersję i, w stosownych przypadkach, wydanie wspólnych kryteriów zastosowanych do oceny;

      2) pakiet dotyczący uzasadnienia zaufania zawarty we wspólnych kryteriach i komponenty uzasadnienia zaufania do bezpieczeństwa, w tym poziom AVA_VAN stosowany podczas oceny oraz odpowiadający mu poziom uzasadnienia zaufania określony w art. 52 rozporządzenia (UE) 2019/881, do którego to poziomu odnosi się certyfikat EUCC;

      3) funkcje bezpieczeństwa ocenionego produktu ICT;

      4) podsumowanie zagrożeń i organizacyjnej polityki bezpieczeństwa, do których odnosi się oceniony produkt ICT;

5) specjalne wymogi dotyczące konfiguracji;

6) założenia dotyczące środowiska operacyjnego;

7) w stosownych przypadkach – obecność zatwierdzonej procedury zarządzania poprawkami zgodnie z sekcją IV.4 załącznika IV;

8) zastrzeżenia prawne.

5. Oceniony produkt ICT musi być jasno wskazany, łącznie z następującymi informacjami:

a) nazwą ocenionego produktu ICT;

b) wyliczeniem komponentów produktu ICT stanowiących część oceny;

c) numerem wersji komponentów produktu ICT;

d) określeniem dodatkowych wymogów środowiska operacyjnego certyfikowanego produktu ICT;

e) imieniem i nazwiskiem lub nazwą oraz danymi kontaktowymi posiadacza certyfikatu EUCC;

f) w stosownych przypadkach – procedurą zarządzania poprawkami ujętą w certyfikacie;

g) linkiem do strony internetowej posiadacza certyfikatu EUCC, która zawiera dodatkowe informacje na temat cyberbezpieczeństwa certyfikowanego produktu ICT zgodnie z art. 55 rozporządzenia (UE) 2019/881.

6. Informacje zawarte w tej sekcji muszą być możliwie dokładne, aby zapewnić pełne i dokładne przedstawienie produktu ICT, które można będzie ponownie wykorzystać w przyszłych ocenach.

7. Sekcja dotycząca polityki bezpieczeństwa zawiera opis polityki bezpieczeństwa produktu ICT oraz polityk lub zasad, których egzekwowaniu oceniony produkt ICT ma służyć lub z którymi musi być zgodny. Sekcja ta zawiera odniesienie do następujących polityk i ich opis:

a) polityki postępowania posiadacza certyfikatu w przypadku wykrycia podatności;

b) polityki ciągłości uzasadnienia zaufania posiadacza certyfikatu.

8. W stosownych przypadkach polityka może obejmować warunki związane ze stosowaniem procedury zarządzania poprawkami w okresie ważności certyfikatu.

9. Sekcja dotycząca założeń i sprecyzowanie zakresu zawiera wyczerpujące informacje dotyczące okoliczności i celów związanych z przewidzianym stosowaniem produktu, o którym to stosowaniu mowa w art. 7 ust. 1 lit. c). Informacje te obejmują:

a) założenia dotyczące stosowania i wdrażania produktu ICT w formie minimalnych wymogów, takich jak spełnienie wymogów dotyczących właściwej instalacji i konfiguracji oraz wymogów sprzętowych;

b) założenia dotyczące środowiska w odniesieniu do zgodnego z wymogami funkcjonowania produktu ICT.

10. Informacje wymienione w pkt 9 muszą być jak najbardziej zrozumiałe, aby umożliwić użytkownikom certyfikowanego produktu ICT podejmowanie świadomych decyzji dotyczących ryzyka związanego z jego stosowaniem.

11. Sekcja informacji dotyczących architektury zawiera szczegółowy opis produktu ICT i jego głównych komponentów zgodnie z projektem podsystemów ADV_TDS w ramach wspólnych kryteriów.

12. Pełny wykaz dodatkowych informacji na temat cyberbezpieczeństwa produktu ICT przedstawia się zgodnie z art. 55 rozporządzenia (UE) 2019/881. Całą odpowiednią dokumentację należy oznaczyć numerami wersji.

13. Sekcja dotycząca badania produktu ICT zawiera następujące informacje:

    a) nazwę i punkt kontaktowy organu lub jednostki, które wydały certyfikat, w tym odpowiedzialnego krajowego organu ds. certyfikacji cyberbezpieczeństwa;

    b) nazwę ITSEF, która przeprowadziła ocenę, jeżeli nie jest to jednostka certyfikująca;

    c) wskazanie wykorzystanych komponentów uzasadnienia zaufania pochodzących z norm, o których mowa w art. 3;

    d) wersję dokumentu odzwierciedlającego stan wiedzy i dalsze kryteria oceny bezpieczeństwa zastosowane w ocenie;

    e) kompletne i precyzyjne ustawienia i konfigurację produktu ICT podczas oceny, w tym uwagi operacyjne i obserwacje, jeżeli są dostępne;

    f) wszelkie zastosowane profile zabezpieczeń, w tym następujące informacje:

        1) autor profilu zabezpieczeń;

        2) nazwa i identyfikator profilu zabezpieczeń;

        3) identyfikator certyfikatu profilu zabezpieczeń;

        4) nazwa i dane kontaktowe jednostki certyfikującej i ITSEF zaangażowanych w ocenę profilu zabezpieczeń;

        5) pakiety dotyczące uzasadnienia zaufania wymagane w przypadku produktu zgodnego z profilem zabezpieczeń.

14. W sekcji zawierającej wyniki oceny i informacje dotyczące certyfikatu znajdują się następujące informacje:

    a) potwierdzenie osiągniętego poziomu uzasadnienia zaufania, o którym mowa w art. 4 niniejszego rozporządzenia oraz w art. 52 rozporządzenia (UE) 2019/881;

    b) wymogi dotyczące uzasadnienia zaufania wynikające z norm, o których mowa w art. 3, faktycznie spełniane przez produkt ICT lub profil zabezpieczeń, w tym poziom AVA_VAN;

    c) szczegółowy opis wymogów dotyczących uzasadnienia zaufania, jak również szczegółowe informacje na temat sposobu, w jaki produkt spełnia każdy z tych wymogów;

    d) data wydania i okres ważności certyfikatu;

    e) niepowtarzalny identyfikator certyfikatu.

15. Cel bezpieczeństwa ujmuje się w sprawozdaniu z certyfikacji lub przywołuje i streszcza w sprawozdaniu z certyfikacji i podaje wraz z powiązanym z nim sprawozdaniem z certyfikacji do celów publikacji.

16. Cel bezpieczeństwa można poddać sanityzacji zgodnie z sekcją VI.2.

17. Znak lub etykieta związane z EUCC można umieścić w sprawozdaniu z certyfikacji zgodnie z zasadami i procedurami określonymi w art. 11.

18. Sekcja poświęcona bibliografii zawiera odniesienia do wszystkich dokumentów wykorzystanych przy sporządzaniu sprawozdania z certyfikacji. Informacje te obejmują co najmniej następujące elementy:

    a) kryteria oceny bezpieczeństwa, dokumenty odzwierciedlające stan wiedzy i inne wykorzystane odpowiednie specyfikacje oraz ich wersję;

    b) sprawozdanie techniczne z oceny;

    c) w stosownych przypadkach – sprawozdanie techniczne z oceny na potrzeby oceny złożonej;

    d) referencyjną dokumentację techniczną;

    e) dokumentację twórcy wykorzystaną w procesie oceny.

19. Aby zagwarantować odtwarzalność oceny, cała przywołana dokumentacja musi być jednoznacznie zidentyfikowana za pomocą właściwej daty wydania i właściwego numeru wersji.

### V.2 **Sanityzacja celu bezpieczeństwa na potrzeby publikacji**

1. Cel bezpieczeństwa, który ujmuje lub przywołuje się w sprawozdaniu z certyfikacji zgodnie z sekcją VI.1 pkt 1, można poddać sanityzacji przez usunięcie lub sparafrazowanie zastrzeżonych informacji technicznych.

2. Otrzymany w ten sposób cel bezpieczeństwa poddany sanityzacji musi być rzeczywistym odzwierciedleniem jego pełnej wersji oryginalnej. Oznacza to, że w celu bezpieczeństwa poddanym sanityzacji nie można pomijać informacji, które są niezbędne do zrozumienia cech bezpieczeństwa celu oceny i zakresu oceny.

3. Treść celu bezpieczeństwa poddanego sanityzacji musi być zgodna z następującymi wymogami minimalnymi:
   a) jego wprowadzenia nie można poddać sanityzacji, ponieważ nie zawiera ono zasadniczo żadnych informacji zastrzeżonych;
   b) cel bezpieczeństwa poddany sanityzacji musi posiadać niepowtarzalny identyfikator, który różni się od identyfikatora jego pełnej wersji oryginalnej;
   c) opis celu oceny można ograniczyć, ponieważ może zawierać on zastrzeżone i szczegółowe informacje na temat projektu celu oceny, które nie powinny być publikowane;
   d) nie można ograniczyć opisu środowiska bezpieczeństwa celu oceny (założeń, zagrożeń, organizacyjnej polityki bezpieczeństwa), o ile informacje te są niezbędne do zrozumienia zakresu oceny;
   e) nie można ograniczyć opisu celów bezpieczeństwa, ponieważ wszystkie informacje mają być podane do wiadomości publicznej na potrzeby zrozumienia intencji celu bezpieczeństwa i celu oceny;
   f) wszystkie wymogi bezpieczeństwa podaje się do wiadomości publicznej. Uwagi dotyczące stosowania mogą zawierać informacje na temat sposobu, w jaki wymogi funkcjonalne wspólnych kryteriów, o których mowa w art. 3, wykorzystano do zrozumienia celu bezpieczeństwa;
   g) streszczenie specyfikacji celu oceny obejmuje wszystkie funkcje bezpieczeństwa celu oceny, ale dodatkowe informacje zastrzeżone można poddać sanityzacji;
   h) podaje się odniesienia do profili zabezpieczeń zastosowanych wobec celu oceny;
   i) uzasadnienie można poddać sanityzacji w celu usunięcia informacji zastrzeżonych.

4. Nawet jeżeli cel bezpieczeństwa poddany sanityzacji nie jest formalnie oceniony zgodnie z normami oceny, o których mowa w art. 3, jednostka certyfikująca zapewnia jego zgodność z pełnym i ocenionym celem bezpieczeństwa oraz przywołuje w sprawozdaniu z certyfikacji zarówno pełny, jak i poddany sanityzacji cel ochrony.

*ZAŁĄCZNIK VI*

**Zakres wzajemnej oceny i skład zespołu na potrzeby wzajemnych ocen**

## VI.1 **Zakres wzajemnej oceny**

1. Uwzględnia się następujące typy wzajemnych ocen:

   a) typ 1: gdy jednostka certyfikująca wykonuje działania w zakresie certyfikacji na poziomie AVA_VAN.3;

   b) typ 2: gdy jednostka certyfikująca wykonuje działania w zakresie certyfikacji związane z domeną techniczną wymienioną w załączniku I jako dokumenty odzwierciedlające stan wiedzy;

   c) typ 3: gdy jednostka certyfikująca wykonuje działania w zakresie certyfikacji powyżej poziomu AVA_VAN.3 z wykorzystaniem profilu zabezpieczeń wymienionego w załączniku II lub III jako dokumenty odzwierciedlające stan wiedzy.

2. Jednostka certyfikująca poddana wzajemnej ocenie przedkłada wykaz certyfikowanych produktów ICT, które mogą być kandydatami do przeprowadzenia przeglądu przez zespół ds. wzajemnej oceny, zgodnie z następującymi zasadami:

   a) produkty będące kandydatami obejmują zakres techniczny zezwolenia jednostki certyfikującej, z czego oceny co najmniej dwóch różnych produktów o poziomie uzasadnienia zaufania „wysoki" zostaną poddane analizie w ramach wzajemnej oceny, oraz jeden profil zabezpieczeń, jeżeli jednostka certyfikująca wydała certyfikat o poziomie uzasadnienia zaufania „wysoki";

   b) w przypadku wzajemnej oceny typu 2 jednostka certyfikująca przedkłada co najmniej jeden produkt dla każdej domeny technicznej i dla każdej zainteresowanej ITSEF;

   c) w przypadku wzajemnej oceny typu 3 co najmniej jeden produkt będący kandydatem ocenia się zgodnie z mającymi zastosowanie i odpowiednimi profilami zabezpieczeń.

## VI.2 **Zespół ds. wzajemnej oceny**

1. Zespół ds. oceny składa się z co najmniej dwóch ekspertów wybranych z różnych jednostek certyfikujących z różnych państw członkowskich, które to jednostki wydają certyfikaty o poziomie uzasadnienia zaufania „wysoki". Eksperci powinni wykazać się odpowiednią wiedzą fachową w zakresie norm, o których mowa w art. 3, oraz dokumentów odzwierciedlających stan wiedzy wchodzących w zakres wzajemnej oceny.

2. W przypadku powierzenia zadania polegającego na wydawaniu certyfikatów lub uprzednim zatwierdzaniu certyfikatów, o czym mowa w art. 56 ust. 6 rozporządzenia (UE) 2019/881, w zespole ekspertów wybranych zgodnie z pkt 1 niniejszej sekcji ponadto uczestniczy ekspert z krajowego organu ds. certyfikacji cyberbezpieczeństwa związany z daną jednostką certyfikującą.

3. Do celów wzajemnej oceny typu 2 członkowie zespołu wybierani są z jednostek certyfikujących posiadających zezwolenie w odniesieniu do danej domeny technicznej.

4. Każdy członek zespołu ds. oceny musi mieć co najmniej dwuletnie doświadczenie w prowadzeniu działań w zakresie certyfikacji w jednostce certyfikującej;

5. W przypadku wzajemnej oceny typu 2 lub 3 każdy członek zespołu ds. oceny musi mieć co najmniej dwuletnie doświadczenie w prowadzeniu działań w zakresie certyfikacji w tej odpowiedniej domenie technicznej lub profilu zabezpieczeń oraz potwierdzoną wiedzę fachową i doświadczenie związane z uczestnictwem w udzieleniu zezwolenia ITSEF.

6. Krajowy organ ds. certyfikacji cyberbezpieczeństwa monitoruje i nadzoruje jednostkę certyfikującą poddaną wzajemnej ocenie, a co najmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa, którego jednostka certyfikująca nie podlega wzajemnej ocenie, uczestniczy we wzajemnej ocenie w charakterze obserwatora. Również ENISA może uczestniczyć we wzajemnej ocenie w charakterze obserwatora.

7. Jednostce certyfikującej poddanej wzajemnej ocenie przedstawia się skład zespołu ds. wzajemnej oceny. W uzasadnionych przypadkach może ona zakwestionować skład zespołu ds. wzajemnej oceny i poprosić o jego przegląd.

*ZAŁĄCZNIK VII*

**Treść certyfikatu EUCC**

Certyfikat EUCC zawiera co najmniej:

a) niepowtarzalny identyfikator nadany przez jednostkę certyfikującą wydającą certyfikat;

b) informacje dotyczące certyfikowanego produktu ICT lub profilu zabezpieczeń oraz posiadacza certyfikatu, w tym:

   1) nazwa produktu ICT lub profilu zabezpieczeń oraz, w stosownych przypadkach, cel oceny;

   2) rodzaj produktu ICT lub profilu zabezpieczeń oraz, w stosownych przypadkach, cel oceny;

   3) wersja produktu ICT lub profilu zabezpieczeń;

   4) imię i nazwisko lub nazwa, adres i dane kontaktowe posiadacza certyfikatu;

   5) link do strony internetowej posiadacza certyfikatu zawierającej dodatkowe informacje na temat cyberbezpieczeństwa, o których mowa w art. 55 rozporządzenia (UE) 2019/881;

c) informacje dotyczące oceny i certyfikacji produktu ICT lub profilu zabezpieczeń, w tym:

   1) nazwa, adres i dane kontaktowe jednostki certyfikującej, która wydała certyfikat;

   2) nazwa ITSEF, która przeprowadziła ocenę, jeżeli nie jest to jednostka certyfikująca;

   3) nazwa odpowiedzialnego krajowego organu ds. certyfikacji cyberbezpieczeństwa;

   4) odniesienie do niniejszego rozporządzenia;

   5) odniesienie do dołączonego do certyfikatu sprawozdania z certyfikacji, o którym mowa w załączniku V;

   6) mający zastosowanie poziom uzasadnienia zaufania zgodnie z art. 4;

   7) odniesienie do wersji norm, o których mowa w art. 3, zastosowanych na potrzeby oceny;

   8) wskazanie pakietu lub poziomu uzasadnienia zaufania określonego w normach, o których mowa w art. 3, oraz zgodnie z załącznikiem VIII, w tym stosowanych komponentów uzasadnienia zaufania i uwzględnionych poziomów AVA_VAN;

   9) w stosownych przypadkach – odniesienie do co najmniej jednego profilu zabezpieczeń, z którym produkt ICT lub profil zabezpieczeń jest zgodny;

   10) data wydania;

   11) okres ważności certyfikatu;

d) znak i etykieta powiązane z certyfikatem zgodnie z art. 11.

*ZAŁĄCZNIK VIII*

**Oświadczenie o pakiecie dotyczącym uzasadnienia zaufania**

1. W przeciwieństwie do definicji zawartych we wspólnych kryteriach rozszerzenie:

a) nie może być oznaczone skrótem „+";

b) musi być szczegółowo opisane w wykazie wszystkich odnośnych komponentów;

c) musi być szczegółowo opisane w sprawozdaniu z certyfikacji.

2. Poziom uzasadnienia zaufania potwierdzony w certyfikacie EUCC można uzupełnić oceną poziomu uzasadnienia zaufania określoną w art. 3 niniejszego rozporządzenia.

3. Jeżeli poziom uzasadnienia zaufania potwierdzony w certyfikacie EUCC nie zawiera odniesienia do rozszerzenia, w certyfikacie EUCC wskazuje się jeden z następujących pakietów:

a) „specjalny pakiet dotyczący uzasadnienia zaufania";

b) „pakiet dotyczący uzasadnienia zaufania zgodny z profilem zabezpieczeń" w przypadku odniesienia do profilu zabezpieczeń bez oceny poziomu uzasadnienia zaufania.

*ZAŁĄCZNIK IX*

**Znak i etykieta**

1. Forma znaku i etykiety:


2. przypadku zmniejszenia lub powiększenia znaku i etykiety zachowuje się proporcje przedstawione na powyższym rysunku.

3. W przypadku fizycznej obecności znak i etykieta muszą mieć co najmniej 5 mm wysokości.