Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2024/3144

19.12.2024

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/3144

z dnia 18 grudnia 2024 r.

w sprawie zmiany rozporządzenia wykonawczego (UE) 2024/482 w odniesieniu do mających zastosowanie norm międzynarodowych i w sprawie sprostowania tego rozporządzenia wykonawczego

(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 rozporządzeniu wykonawczym Komisji (UE) 2024/482 ([2]) 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.

(2) Rozporządzenie wykonawcze (UE) 2024/482 opiera się na ugruntowanych normach międzynarodowych, którymi są wspólne kryteria i wspólna metodyka oceny utrzymywane przez Międzynarodową Organizację Normalizacyjną (ISO) i Międzynarodową Komisję Elektrotechniczną (IEC). W rozporządzeniu wykonawczym (UE) 2024/482 zawarto odniesienie do norm ISO/IEC, ale nie określono w nim mającej zastosowanie wersji tych norm. Należy zatem określić, która wersja norm ma zastosowanie do certyfikatów wydawanych na podstawie EUCC.

(3) Organizacje rządowe, które przyczyniły się do opracowania wspólnych kryteriów i wspólnej metodyki oceny w drodze Porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego (CCRA), są współwłaścicielami, wraz z ISO/IEC, praw autorskich do nich. Te organizacje rządowe zachowują prawo do korzystania z nich. Ze względu na znaczenie tych dokumentów wywodzących się z CCRA powinny one również stanowić podstawę certyfikacji na podstawie EUCC.

(4) Normy dotyczące wspólnych kryteriów i wspólnej metodyki oceny podlegają interpretacjom dokonywanym przez CCRA, które ułatwiają ich wdrożenie i które mogą zostać uwzględnione przez jednostki oceniające bezpieczeństwo technologii informacyjnych (ITSEF) oraz jednostki certyfikujące.

(5) Normy międzynarodowe odnoszące się do wspólnych kryteriów mogą podlegać aktualizacji. Aby zapewnić uporządkowane i terminowe przejście, należy określić przepisy przejściowe w celu zapewnienia sprzedawcom, ITSEF i jednostkom certyfikującym oraz innym odpowiednim podmiotom wystarczającej ilości czasu na niezbędne dostosowania. Przepisy przejściowe powinny być w odpowiednim stopniu dostosowane do praktyk globalnych, takich jak te określone w CCRA.

([1]) Dz.U. L 151 z 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

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

(6) W rozporządzeniu wykonawczym (UE) 2024/482 nie określono, do kiedy certyfikacja produktu ICT może się opierać na poprzednich wersjach norm dotyczących wspólnych kryteriów i wspólnej metodyki oceny. Domeny techniczne i profile zabezpieczeń wymienione w załącznikach I, II i III do wspomnianego rozporządzenia wykonawczego opierają się na poprzednich wersjach norm ISO/IEC 15408 i 18045. W rozporządzeniu wykonawczym (UE) 2024/482 trzeba zatem określić, w jakich okolicznościach należy kontynuować stosowanie poprzedniej wersji wspólnych kryteriów i wspólnej metodyki oceny oraz w jaki sposób nastąpi przejście na najnowszą wersję norm międzynarodowych.

(7) W okresie przejściowym aktualizacja odpowiednich domen technicznych i profili zabezpieczeń powinna być priorytetem dla odpowiednich zainteresowanych stron. W rozporządzeniu wykonawczym (UE) 2024/482 należy przewidzieć, że cele w zakresie bezpieczeństwa oparte na poprzedniej wersji norm będą akceptowane do 31 grudnia 2027 r. zgodnie z polityką transformacji przyjętą w CCRA. Należy jednak zauważyć, że polityka transformacji CCRA obejmuje wstępne oceny produktów i profili zabezpieczeń rozpoczynające się nie później niż 30 czerwca 2024 r., kiedy to EUCC nie miał jeszcze zastosowania. Ponadto zgodnie z polityką transformacji CCRA w rozporządzeniu wykonawczym (UE) 2024/482 należy przewidzieć, że cele w zakresie bezpieczeństwa zgodne z tym rozporządzeniem wykonawczym, stwierdzające zgodność z profilami zabezpieczeń opartymi na poprzedniej wersji norm, będą akceptowane do 31 grudnia 2027 r. Ponadto w przypadku wydania nowego certyfikatu na podstawie rozporządzenia wykonawczego (UE) 2024/482 w kontekście procesu przeglądu certyfikatu krajowego, który rozpoczyna się w ciągu dwóch lat od wydania pierwotnego certyfikatu, powinna istnieć możliwość korzystania z poprzedniej wersji norm. Nie miałoby to znaczenia dla procesu przeglądu, który nie wymaga wydania nowego certyfikatu na podstawie rozporządzenia wykonawczego (UE) 2024/482, i w przypadku gdy certyfikat pozostaje ważny.

(8) W celu zapewnienia uporządkowanego przejścia na najnowszą wersję norm w rozporządzeniu wykonawczym (UE) 2024/482 należy przewidzieć szczegółowe przepisy przejściowe i nadal umożliwiać wydawanie certyfikatów na podstawie tego rozporządzenia wykonawczego stwierdzających zgodność z profilami zabezpieczeń opartymi na poprzednich wersjach norm opublikowanych przez CCRA, w przypadku gdy stosowanie takich profili zabezpieczeń jest wymagane na mocy przepisów Unii. Tak jest w przypadku rozporządzenia wykonawczego Komisji (UE) 2016/799 ([3]) oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([4]) i decyzji wykonawczej Komisji (UE) 2016/650 ([5]).

(9) W załączniku I do rozporządzenia wykonawczego (UE) 2024/482 wymieniono mające zastosowanie dokumenty odzwierciedlające stan wiedzy do celów oceny produktów ICT i profili zabezpieczeń. Nie określono w nim jednak wersji tych dokumentów. Należy zatem określić, która wersja dokumentów ma zastosowanie do certyfikatów wydawanych na podstawie EUCC. Wersje te opierają się na dokumentach zatwierdzonych przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa (ECCG), a jednocześnie zostały poddane dalszemu przeglądowi w celu ich uwzględnienia w EUCC. Ponadto należy zmienić załącznik I, aby uwzględnić zaktualizowane i nowe dokumenty odzwierciedlające stan wiedzy po ich zatwierdzeniu przez ECCG, zapewniając w ten sposób jednolitą akredytację jednostek oceniających zgodność w ramach EUCC. Należy zaktualizować wymogi akredytacji związane z akredytacją ITSEF w celu wyjaśnienia stosowania kryteriów niezależności i bezstronności oraz ustanowić nowy dokument odzwierciedlający stan wiedzy dotyczący akredytacji jednostek certyfikujących.

(10) Dokumenty odzwierciedlające stan wiedzy mogą być dodawane do EUCC lub mogą podlegać aktualizacji w kontekście jego działań związanych z utrzymaniem. W przypadku nowych lub zaktualizowanych dokumentów odzwierciedlających stan wiedzy konieczne może być ustanowienie odpowiednich przepisów przejściowych, aby umożliwić sprzedawcom, ITSEF, jednostkom certyfikującym i innym zainteresowanym stronom dokonanie niezbędnych dostosowań. W przypadku aktualizacji dokumentu odzwierciedlającego aktualny stan wiedzy związanego z akredytacją ITSEF zaktualizowany dokument powinien mieć zastosowanie do akredytacji wydanych przed dniem 8 lipca 2025 r. wyłącznie w przypadku ich przeglądu, np. w kontekście procedury oceny lub ponownej oceny. Ponadto zaktualizowany dokument powinien mieć zastosowanie do wszystkich akredytacji ITSEF wydanych po dniu 8 lipca 2025 r.

([3]) Rozporządzenie wykonawcze Komisji (UE) 2016/799 z dnia 18 marca 2016 r. w sprawie wykonania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 165/2014 ustanawiającego wymogi dotyczące budowy, sprawdzania, instalacji, użytkowania i naprawy tachografów oraz ich elementów składowych (Dz.U. L 139 z 26.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Decyzja wykonawcza Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiająca normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U. L 109 z 26.4.2016, s. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Dodatkowe sprostowania art. 5, 8, 16, 29 i 44 oraz załącznika IV do rozporządzenia wykonawczego (UE) 2024/482 przyczyniają się do zapewnienia jednolitego brzmienia i jasnej wykładni prawnej.

(12) Zasady notyfikacji jednostek oceniających zgodność należy ustanowić horyzontalnie dla wszystkich systemów objętych europejskimi ramami certyfikacji cyberbezpieczeństwa. Rozporządzenie wykonawcze Komisji (UE) 2024/3143 ([6]) obejmuje te zasady notyfikacji. W związku z powyższym art. 23 i 24 rozporządzenia wykonawczego (UE) 2024/482 należy uchylić od dnia rozpoczęcia stosowania rozporządzenia wykonawczego (UE) 2024/3143.

(13) Należy zatem odpowiednio zmienić i sprostować rozporządzenie wykonawcze (UE) 2024/482.

(14) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na mocy art. 66 rozporządzenia (UE) 2019/881,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

W rozporządzeniu wykonawczym (UE) 2024/482 wprowadza się następujące zmiany:

1) art. 2 pkt 1 i 2 otrzymują brzmienie:

„1) »wspólne kryteria« oznaczają wspólne kryteria oceny bezpieczeństwa technologii informacyjnych określone w normach ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 lub ISO/IEC 15408-5:2022 lub określone we wspólnych kryteriach oceny bezpieczeństwa technologii informacyjnych, wersja CC:2022, części 1–5, opublikowanych przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego;

2) »wspólna metodyka oceny« oznacza wspólną metodykę oceny bezpieczeństwa technologii informacyjnych określoną w normie ISO/IEC 18045:2022 lub wspólną metodykę oceny bezpieczeństwa technologii informacyjnych, wersja CEM:2022, opublikowaną przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego;";

2) art. 3 otrzymuje brzmienie:

„*Artykuł 3*

Normy dotyczące oceny

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

a) wspólne kryteria;

b) wspólna metodyka oceny.

2. Do dnia 31 grudnia 2027 r. certyfikat może być wydawany w ramach programu EUCC z zastosowaniem jednej z następujących norm:

a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 lub ISO/IEC 15408-3:2008;

b) wspólnych kryteriów oceny bezpieczeństwa technologii informacyjnych, wersja 3.1, poprawka 5, opublikowanych przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego;

([6]) Rozporządzenie wykonawcze Komisji (UE) 2024/3143 z dnia 18 grudnia 2024 r. ustanawiające okoliczności, formaty i procedury dotyczące notyfikacji zgodnie z art. 61 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (Dz.U. L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/IEC 18045:2008;

d) wspólnej metodyki oceny bezpieczeństwa technologii informacyjnych, wersja 5, poprawka 3.1, opublikowanej przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego;

3. Do dnia 31 grudnia 2027 r. w ramach programu EUCC można wydawać certyfikat zgodny z normami, o których mowa w ust. 1, stwierdzający zgodność z profilem zabezpieczeń, w którym zastosowano normy wymienione w ust. 2.

4. Certyfikat zgodny z normami, o których mowa w ust. 1, może być również wydawany w ramach programu EUCC potwierdzającego zgodność z profilem zabezpieczeń, w którym zastosowano którąkolwiek z poniższych norm, pod warunkiem że stosowanie takiego profilu zabezpieczeń jest wymagane na mocy rozporządzenia wykonawczego Komisji (UE) 2016/799 (*), rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 (**) lub decyzji wykonawczej Komisji (UE) 2016/650 (***):

a) wspólne kryteria oceny bezpieczeństwa technologii informacyjnych, wersja 3.1, poprawka 1–4, opublikowane przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego;

b) wspólna metodyka oceny bezpieczeństwa technologii informacyjnych, wersja 3.1, poprawka 1–4, opublikowana przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego;

(*) Rozporządzenie wykonawcze Komisji (UE) 2016/799 z dnia 18 marca 2016 r. w sprawie wykonania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 165/2014 ustanawiającego wymogi dotyczące budowy, sprawdzania, instalacji, użytkowania i naprawy tachografów oraz ich elementów składowych (Dz.U. L 139 z 26.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Decyzja wykonawcza Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiająca normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U. L 109 z 26.4.2016, s. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).";

3) w rozdziale IV dodaje się art. 20a w brzmieniu:

„*Artykuł 20a*

Specyfikacja wymagań w zakresie akredytacji jednostek oceniających zgodność

Akredytacja jednostek oceniających zgodność musi uwzględniać specyfikację wymogów dotyczących akredytacji jednostek certyfikujących oraz ITSEF, określonych w mających zastosowanie dokumentach odzwierciedlających aktualny stan wiedzy wymienionych w załączniku I pkt 2.";

4) uchyla się art. 23 i 24;

5) w art. 48 dodaje się ust. 4 w brzmieniu:

„4. O ile w załączniku I lub II nie określono inaczej, dokumenty odzwierciedlające stan wiedzy stosuje się od dnia rozpoczęcia stosowania aktu zmieniającego, na mocy którego zostały one włączone do załącznika I lub II.";

6) w art. 49 dodaje się ust. 4 w brzmieniu:

„4. Przy przeprowadzaniu przeglądu, o którym mowa w ust. 3, w ciągu dwóch lat od wydania pierwotnego certyfikatu i w przypadku gdy taki przegląd prowadzi do wydania nowego certyfikatu zgodnie z niniejszym rozporządzeniem, można stosować normy wymienione w art. 3 ust. 2. Za datę wydania pierwotnego certyfikatu uznaje się datę wydania ostatniego certyfikatu dla produktu ICT lub profilu zabezpieczeń, na którym opiera się obecna certyfikacja.";

7) załącznik I zastępuje się tekstem znajdującym się w załączniku I do niniejszego rozporządzenia;

8) w załączniku IV wprowadza się zmiany zgodnie z załącznikiem II do niniejszego rozporządzenia.

Artykuł 2

W rozporządzeniu wykonawczym (UE) 2024/482 wprowadza się następujące sprostowania:

1) art. 5 ust. 1 lit. b) otrzymuje brzmienie:

„b) przez stwierdzenie zgodności z certyfikowanym profilem zabezpieczeń w ramach procesu ICT, w przypadku gdy produkt ICT należy do kategorii produktów ICT objętej tym profilem zabezpieczeń.";

2) w art. 8 wprowadza się następujące sprostowania:

a) tytuł otrzymuje brzmienie:

„Informacje niezbędne do certyfikacji i oceny";

b) ust. 1 otrzymuje brzmienie:

„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 i oceny.";

3) art. 16 otrzymuje brzmienie:

„*Artykuł 16*

Informacje niezbędne do certyfikacji i oceny 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 i oceny w pełnej i prawidłowej formie. Art. 8 ust. 2, 3, 4 i 7 stosuje się odpowiednio.";

4) w art. 17 uchyla się ust. 1;

5) art. 29 ust. 2 otrzymuje brzmienie:

„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 lub art. 20.";

Artykuł 3

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

Art. 1 ust. 4 stosuje się od dnia 8 stycznia 2025 r.

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

Sporządzono w Brukseli dnia 18 grudnia 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

„„ZAŁĄCZNIK I

Dokumenty odzwierciedlające stan wiedzy potwierdzające domeny techniczne i inne dokumenty odzwierciedlające stan wiedzy

1. Dokumenty odzwierciedlające stan wiedzy potwierdzające domeny techniczne na poziomie AVA_VAN 4 lub 5:

   a) następujące dokumenty dotyczące zharmonizowanej oceny domeny technicznej »karty elektroniczne i podobne urządzenia«:

      1) »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« [»Minimalne wymogi ITSEF dotyczące oceny bezpieczeństwa kart elektronicznych i podobnych urządzeń«], wersja 1.1;

      2) »Minimum Site Security Requirements« [»Minimalne wymogi bezpieczeństwa obiektu«], wersja 1.1;

      3) »Application of Common Criteria to integrated circuits« [»Zastosowanie wspólnych kryteriów do układów scalonych«], wersja 1.1;

      4) »Security Architecture requirements (ADV_ARC) for smart cards and similar devices« [»Wymogi architektury bezpieczeństwa (ADV_ARC) dotyczące kart elektronicznych i podobnych urządzeń«], wersja 1.1;

      5) »Certification of 'open' smart card products« [»Certyfikacja 'otwartych' produktów kart elektronicznych«], wersja 1.1;

      6) »Composite product evaluation for smart cards and similar devices« [»Ocena produktu złożonego w przypadku kart elektronicznych i podobnych urządzeń«], wersja 1.1;

      7) »Application of Attack Potential to Smartcards and Similar Devices« [»Zastosowanie potencjału ataku do kart elektronicznych i podobnych urządzeń«], wersja 1.2.

   b) następujące dokumenty dotyczące zharmonizowanej oceny domeny technicznej »urządzenia sprzętowe ze skrzynkami bezpieczeństwa«:

      1) »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« [»Minimalne wymogi ITSEF dotyczące oceny bezpieczeństwa urządzeń sprzętowych ze skrzynkami bezpieczeństwa«], wersja 1.1;

      2) »Minimum Site Security Requirements« [»Minimalne wymogi bezpieczeństwa obiektu«], wersja 1.1;

      3) »Application of Attack Potential to hardware devices with security boxes« [»Zastosowanie potencjału ataku do urządzeń sprzętowych ze skrzynkami bezpieczeństwa«], wersja 1.2.

2. Dokumenty odzwierciedlające stan wiedzy związane ze zharmonizowaną akredytacją jednostek oceniających zgodność:

   a) »Accreditation of ITSEFs for the EUCC« [»Akredytacja ITSEF dla EUCC«], wersja 1.1 w odniesieniu do akredytacji wydanych przed dniem 8 lipca 2025 r.;

   b) »Accreditation of ITSEFs for the EUCC« [»Akredytacja ITSEF dla EUCC«], wersja 1.6c w odniesieniu do nowo wydanych akredytacji lub akredytacji poddanych przeglądowi po dniu 8 lipca 2025 r.;

   c) »Accreditation of CBs for the EUCC« [»Akredytacja jednostek certyfikujących dla EUCC«], wersja 1.6b.”.”

ZAŁĄCZNIK II

W załączniku IV do rozporządzenia wykonawczego (UE) 2024/482 sekcja IV.3 pkt 5 i 6 otrzymują brzmienie:

„5. W przypadku gdy jednostka certyfikująca potwierdziła, że zmiany są nieistotne, nie wydaje się nowego certyfikatu dla zmienionego produktu ICT oraz sporządza się sprawozdanie z utrzymania dotyczące pierwotnego sprawozdania z certyfikacji.

Sprawozdanie z utrzymania ujmuje się jako podzbiór sprawozdania z analizy skutków, zawierający następujące sekcje:

a) wprowadzenie;

b) opis zmian;

c) dowody twórcy, na które zmiany mają wpływ.

6. Sprawozdanie z utrzymania, o którym mowa w pkt 5, przekazuje się ENISA do publikacji na jej stronie internetowej poświęconej certyfikacji cyberbezpieczeństwa.”.