2024/2981

4.12.2024

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/2981

z dnia 28 listopada 2024 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do certyfikacji europejskich portfeli tożsamości cyfrowej

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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 ([1]), w szczególności jego art. 5c ust. 6,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 5c rozporządzenia (UE) nr 910/2014 certyfikację europejskich portfeli tożsamości cyfrowej („portfele") należy przeprowadzać zgodnie z wymogami funkcjonalnymi oraz wymogami związanymi z cyberbezpieczeństwem i ochroną danych, aby zapewnić wysoki poziom bezpieczeństwa i zaufania do portfeli. Te wymogi w zakresie certyfikacji należy zharmonizować we wszystkich państwach członkowskich, aby zapobiec fragmentacji rynku i stworzyć solidne ramy.

(2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([2]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([3]) mają zastosowanie do czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

(3) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm lub specyfikacji technicznych. Aby zapewnić maksymalną harmonizację działań państw członkowskich w zakresie opracowywania i certyfikacji portfeli, specyfikacje techniczne określone w niniejszym rozporządzeniu opierają się na pracach przeprowadzonych na podstawie zalecenia Komisji (UE) 2021/946 z dnia 3 czerwca 2021 r. w sprawie wspólnego unijnego zestawu narzędzi na potrzeby skoordynowanego podejścia do europejskich ram tożsamości cyfrowej ([4]), a w szczególności architektury i ram odniesienia, które są jego częścią. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 ([5]) Komisja powinna, w razie potrzeby, poddawać niniejsze rozporządzenie wykonawcze przeglądowi i aktualizacji, aby zachować aktualność względem globalnych zmian, architektury i ram odniesienia oraz przestrzegać najlepszych praktyk na rynku wewnętrznym.

(4) W celu poświadczenia zgodności z wymogami związanymi z cyberbezpieczeństwem zawartymi w ramach certyfikacji certyfikacja rozwiązań w zakresie portfela powinna odnosić się, w miarę dostępności i w stosownych przypadkach, do europejskich programów certyfikacji cyberbezpieczeństwa ustanowionych na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 ([6]). W przypadku braku takich programów lub w sytuacji, gdy tylko częściowo spełniają one wymogi związane z cyberbezpieczeństwem, niniejsze rozporządzenie ustanawia wymogi ogólne mające zastosowanie do krajowych programów certyfikacji, uwzględniając wymogi funkcjonalne oraz wymogi związane z cyberbezpieczeństwem i ochroną danych.

([1]) Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) Dz.U. L 210 z 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz.U. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

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

(5) Na podstawie art. 5a ust. 11 rozporządzenia (UE) nr 910/2014 portfele muszą być certyfikowane na wysokim poziomie bezpieczeństwa zgodnie z rozporządzeniem (UE) nr 910/2014 oraz rozporządzeniem wykonawczym Komisji (UE) 2015/1502 ([7]). Poziom bezpieczeństwa musi zostać osiągnięty przez rozwiązanie w zakresie portfela w ujęciu ogólnym. Na podstawie niniejszego rozporządzenia niektóre komponenty rozwiązania w zakresie portfela mogą być certyfikowane na niższym poziomie bezpieczeństwa, pod warunkiem że jest to należycie uzasadnione i odbywa się bez uszczerbku dla wysokiego poziomu bezpieczeństwa osiągniętego przez rozwiązanie w ujęciu ogólnym.

(6) Wszystkie krajowe programy certyfikacji powinny wyznaczyć właściciela programu, który będzie odpowiedzialny za opracowanie i utrzymanie programu certyfikacji. Właścicielem programu może być jednostka oceniająca zgodność, organ rządowy lub władza publiczna, organizacja gospodarcza, grupa jednostek oceniających zgodność lub jakikolwiek właściwy organ, który może być inny niż jednostka prowadząca krajowy program certyfikacji.

(7) Przedmiot certyfikacji powinien obejmować komponenty oprogramowania rozwiązania w zakresie portfela, takie jak instancja portfela. Bezpieczna aplikacja kryptograficzna portfela („WSCA"), bezpieczne urządzenie kryptograficzne portfela („WSCD") oraz platformy, na których wykonywane są te komponenty oprogramowania, mimo że są częścią środowiska operacyjnego, powinny być uwzględnione jako przedmiot certyfikacji tylko w sytuacji, gdy są dostarczane przez rozwiązanie w zakresie portfela. W innych przypadkach, w szczególności gdy wskazane urządzenia i platformy są dostarczane przez użytkowników końcowych, dostawcy powinni ustalić założenia dotyczące środowiska operacyjnego rozwiązania w zakresie portfela, w tym na tych urządzeniach i platformach, oraz wdrożyć środki w celu potwierdzenia, że założenia te są weryfikowane w praktyce. W celu zapewnienia ochrony aktywów krytycznych za pomocą sprzętu i oprogramowania systemowego służących do zarządzania kluczami kryptograficznymi tworzonymi, przechowywanymi lub przetwarzanymi przez WSCD oraz do ochrony takich kluczy WSCD musi spełniać wysokie standardy certyfikacji odzwierciedlone w normach międzynarodowych, takie jak wspólne kryteria („EUCC") ustanowione w rozporządzeniu wykonawczym Komisji (UE) 2024/482 ([8]), oceny bezpieczeństwa technologii informacyjnych EAL4 oraz zaawansowana metodyczna ocena podatności na zagrożenia, np. porównywalna z AVA_VAN.5. Z tych norm w zakresie certyfikacji należy skorzystać najpóźniej w chwili przeprowadzania certyfikacji zgodności portfeli zgodnie z europejskim programem certyfikacji cyberbezpieczeństwa przyjętym na podstawie rozporządzenia (UE) 2019/881.

(8) W pełni mobilne, bezpieczne i przyjazne dla użytkownika portfele wspierane dostępnością znormalizowanych i certyfikowanych rozwiązań odpornych na manipulacje, takich jak wbudowane bezpieczne elementy, urządzenia zewnętrzne, np. inteligentne karty, lub wbudowane platformy SIM w urządzeniach mobilnych. Ważną kwestią jest zapewnienie dostępu w wymaganym czasie do wbudowanych bezpiecznych elementów dla krajowych środków eID i portfeli oraz koordynacja starań w tej dziedzinie przez państwa członkowskie. Grupa współpracy na rzecz europejskiej tożsamości cyfrowej ustanowiona na podstawie art. 46e ust. 1 rozporządzenia (UE) nr 910/2014 („grupa współpracy") powinna zatem utworzyć podgrupę do tego celu. Prowadząc konsultacje z odpowiednimi zainteresowanymi stronami, podgrupa ta powinna uzgodnić wspólny plan działania na rzecz dostępu do wbudowanych bezpiecznych elementów, który zostałby uwzględniony przez Komisję na potrzeby sprawozdania z przeglądu dotyczącego rozporządzenia (UE) nr 910/2014. W celu ułatwienia upowszechniania się portfela na poziomie krajowym Komisja powinna ponadto, we współpracy z państwami członkowskimi, opracować i stale aktualizować instrukcję dotycząca przypadków użycia będącą elementem architektury i ram odniesienia.

(9) Przedmiot certyfikacji krajowych programów certyfikacji powinien również obejmować procesy wykorzystywane do zapewnienia i obsługi rozwiązania w zakresie portfela, nawet jeżeli określenie lub wykonanie tych procesów zleca się osobom trzecim. Aby wykazać, że procesy spełniają wymagania programów, dozwolone jest wykorzystanie w ramach dowodu informacji na temat bezpieczeństwa, pod warunkiem że przeprowadzona zostanie analiza zależności w celu ustalenia, czy informacje na temat bezpieczeństwa są wystarczające. Informacje na temat bezpieczeństwa mogą mieć różne formy, takie jak sprawozdania i certyfikaty zgodności, które mogą być wydawane na poziomie prywatnym, krajowym, europejskim lub międzynarodowym na podstawie norm lub specyfikacji technicznych. Celem analizy zależności jest ocena jakości dostępnych informacji na temat bezpieczeństwa komponentów portfela.

([7]) Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 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 235 z 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) 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/2024/482/oj).

(10) Zgodnie z procedurami ustanowionymi w tym celu grupa współpracy powinna mieć możliwość wydawania opinii i zaleceń dotyczących przedkładanych jej projektów krajowych programów certyfikacji. Krajowe programy certyfikacji powinny być dostosowane do architektury portfela, a na potrzeby każdej obsługiwanej architektury powinny być opracowane szczegółowe profile.

(11) W celu zapewnienia wspólnego zrozumienia oraz zharmonizowanego podejścia do oceny najważniejszych rodzajów ryzyka mogących wpłynąć na zapewnianie i obsługę portfeli, należy opracować rejestr ryzyka i zagrożeń, które należy wziąć pod uwagę na etapie opracowywania rozwiązań w zakresie portfela, niezależnie od ich konkretnej architektury. Przy określaniu rodzajów ryzyka, które należy uwzględnić w rejestrze, warto mieć na uwadze cele w zakresie cyberbezpieczeństwa opisane w rozporządzeniu (UE) nr 910/2014, takie jak poufność, integralność i dostępność rozwiązania w zakresie portfela, jak również prywatność użytkowników i danych. Należyte uwzględnienie ryzyka i zagrożeń ujętych w tym rejestrze ryzyka powinno być jednym z wymogów krajowych programów certyfikacji. Aby zachować aktualność względem stale zmieniającego się krajobrazu zagrożeń, rejestr ryzyka powinien być prowadzony i regularnie aktualizowany we współpracy z grupą współpracy.

(12) Ustanawiając swoje programy certyfikacji, właściciele programów powinni przeprowadzić ocenę ryzyka w celu udoskonalenia i uzupełnienia wykazu ryzyka i zagrożeń w rejestrze o ryzyko i zagrożenia charakterystyczne dla architektury lub wdrażania danego rozwiązania w zakresie portfela. W ocenie ryzyka należy uwzględniać, w jaki sposób można odpowiednio zarządzać stosownymi rodzajami ryzyka i zagrożeniami. Dostawcy portfela powinni uzupełnić ocenę ryzyka programu w celu zidentyfikowania wszelkich rodzajów ryzyka i zagrożeń związanych z ich wdrażaniem oraz zaproponować odpowiednie środki zaradcze do oceny przez jednostkę certyfikującą.

(13) Aby wykazać, że architektura rozwiązania w zakresie portfela spełnia obowiązujące wymogi bezpieczeństwa, każdy program lub profil charakterystyczny dla danej architektury powinien zawierać co najmniej opis architektury rozwiązania w zakresie portfela, wykaz wymogów bezpieczeństwa mających zastosowanie do architektury rozwiązania w zakresie portfela, plan oceny w celu potwierdzenia, że rozwiązanie w zakresie portfela oparte na tej architekturze spełnia wskazane wymogi, oraz ocenę ryzyka. Krajowe programy certyfikacji powinny wymagać od dostawców portfela wykazania, w jaki sposób projekt rozwiązania w zakresie portfela, który oferują, odpowiada architekturze odniesienia, oraz szczegółowego opisania zabezpieczeń i planów walidacji dla konkretnego rozwiązania w zakresie portfela. Krajowe programy certyfikacji powinny również określać działanie w zakresie oceny zgodności w celu zweryfikowania, czy projekt portfela właściwie odzwierciedla architekturę odniesienia wybranego profilu. Krajowe programy certyfikacji powinny spełniać wymogi określone w art. 51 rozporządzenia (UE) 2019/881, z wyjątkiem lit. e) i f), w zakresie rejestrowania.

(14) W odniesieniu do certyfikacji produktów należy zezwolić na stosowanie certyfikatów zgodności wydanych w ramach europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach („EUCC") oraz certyfikatów zgodności wydanych w ramach krajowych programów certyfikacji w kontekście umowy o wzajemnym uznawaniu Komitetu Doradczego ds. Bezpieczeństwa Systemów Informatycznych (SOG-IS). Ponadto należy zezwolić na stosowanie innych krajowych programów certyfikacji w odniesieniu do mniej wrażliwych komponentów produktu, takich jak te ustanowione zgodnie z normą CEN EN 17640 w odniesieniu do metod oceny cyberbezpieczeństwa w ustalonym przedziale czasu.

(15) Unijny znak zaufania dla portfela tożsamości cyfrowej („znak zaufania") powinien być stosowany w celu wskazania w jasny, prosty i rozpoznawalny sposób, że portfel został zapewniony zgodnie z rozporządzeniem (UE) nr 910/2014. W związku z tym należy go uznać za znak zgodności dla rozwiązania w zakresie portfela certyfikowanego w ramach krajowych programów certyfikacji. Krajowe programy certyfikacji nie powinny określać żadnych innych znaków zgodności.

(16) Aby zniechęcać do oszustw, krajowe programy certyfikacji powinny określić działania, które należy podjąć w przypadku nieuczciwego wystąpienia o certyfikację w ramach programu.

(17) W celu zapewnienia efektywnego zarządzania notyfikacjami o podatnościach na zagrożenia dostawcy rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, powinni określić i wdrożyć procedury oceny wagi oraz potencjalnego wpływu podatności na zagrożenia. Krajowe programy certyfikacji powinny określać próg, po przekroczeniu którego jednostka certyfikująca ma być notyfikowana. Taki wymóg notyfikacji nie powinien mieć jednak wpływu na kryteria ustanowione w przepisach o ochronie danych oraz przez organy ochrony danych w państwach członkowskich w kontekście notyfikowania naruszeń ochrony danych osobowych. Istnieje możliwość uzyskania synergii pomiędzy obowiązkiem notyfikowania naruszeń bezpieczeństwa lub kompromitacji rozwiązań w zakresie portfela a notyfikowaniem przypadków naruszenia ochrony danych osobowych zgodnie z rozporządzeniem (UE) 2016/679. Przeprowadzona przez jednostkę certyfikującą ewaluacja sprawozdania z oceny skutków podatności na zagrożenia powinna pozostawać bez uszczerbku dla dokonanej przez organ ochrony danych oceny skutków dla ochrony danych zgodnie z art. 35 i 36 rozporządzenia (UE) 2016/679.

(18) Dostawcy rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, powinni notyfikować właścicielowi programu wszelkie uzasadnienia wyjątków od oceny podatności na zagrożenia wymaganej do oceny WSCD i WSCA, jak określono w załączniku IV.

(19) Odwołanie certyfikatu zgodności może mieć poważne konsekwencje, takie jak unieważnienie wszystkich wprowadzonych jednostek portfela. W związku z tym jednostki certyfikujące powinny rozważać odwołanie tylko w sytuacji, gdy nieusunięta podatność na zagrożenia może znacząco wpłynąć na niezawodność danego rozwiązania w zakresie portfela lub innego rozwiązania w zakresie portfela.

(20) Należy wdrożyć specjalną procedurę aktualizacji krajowych programów certyfikacji, aby zarządzać przejściem między kolejnymi wersjami tych programów, szczególnie w kontekście działań, jakie posiadacz certyfikatu powinien podjąć w związku z nadchodzącymi ocenami, utrzymaniem, ponowną certyfikacją oraz ocenami specjalnymi.

(21) Aby ułatwić zapewnianie przejrzystości, dostawcy portfela powinni publicznie udostępniać informacje dotyczące bezpieczeństwa swojego rozwiązania w zakresie portfela.

(22) W przypadku gdy krajowe programy certyfikacji polegają na informacjach na temat bezpieczeństwa pochodzących z innych programów lub źródeł certyfikacji, należy przeprowadzić analizę zależności w celu zweryfikowania, czy dokumentacja bezpieczeństwa, na przykład sprawozdania dotyczące bezpieczeństwa i certyfikaty zgodności, jest dostępna i odpowiednia dla danych rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane. Podstawą takiej analizy zależności powinna być ocena ryzyka związanego z rozwiązaniami w zakresie portfela oraz systemem identyfikacji elektronicznej, w ramach którego są one zapewniane. W ramach oceny należy ustalić, czy dokumentacja bezpieczeństwa dostępna dla danego rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego jest ona zapewniana, jest odpowiednia do zapewniania pewności odpowiadającej poziomowi ukierunkowanej oceny. W ramach oceny należy również zaktualizować analizę zależności lub, w razie potrzeby, dokonać ponownej pełnej oceny.

(23) Jednostki certyfikujące powinny wydawać certyfikaty zgodności w krajowych programach certyfikacji wraz z ogólnodostępnym raportem z certyfikacji, o którym mowa w art. 5d ust. 2 lit. a) rozporządzenia (UE) nr 910/2014. Powiązane sprawozdanie z oceny certyfikacji powinno zostać udostępnione grupie współpracy.

(24) Krajowe programy certyfikacji powinny określać roczną ocenę nadzoru w celu zapewnienia skutecznego funkcjonowania procedur związanych z zarządzaniem portfelami i ich utrzymaniem, czyli zapewnić, aby funkcjonowały one zgodnie z definicją zawartą w zasadach określających te procesy. Ocena podatności na zagrożenia, przeprowadzana raz na dwa lata, jest wymogiem wynikającym z rozporządzenia (UE) nr 910/2014 i ma ona na celu zapewnienie, aby rozwiązanie w zakresie portfela w dalszym ciągu odpowiednio uwzględniało ryzyka w cyberprzestrzeni i zagrożenia cyberbezpieczeństwa zidentyfikowane w rejestrze ryzyka, w tym wszelkie zmiany krajobrazu zagrożeń. Pojęcia „ocena nadzoru", „ocena do celów ponownej certyfikacji" i „ocena specjalna" powinny być zgodne z normą EN ISO/IEC 17021-1:2015.

(25) Cykl certyfikacji kończy się wraz z wygaśnięciem certyfikatu zgodności lub wydaniem nowego certyfikatu zgodności w następstwie pomyślnego wyniku oceny do celów ponownej certyfikacji. Ocena do celów ponownej certyfikacji powinna obejmować ocenę wszystkich komponentów przedmiotu certyfikacji, w tym ocenę skuteczności oraz, w stosownych przypadkach, ocenę podatności na zagrożenia. Podczas ponownej certyfikacji powinno być możliwe ponowne wykorzystanie wyników wcześniejszych ocen dla komponentów, w przypadku których nie miały miejsca żadne zmiany.

(26) Po przyjęciu europejskiego programu certyfikacji cyberbezpieczeństwa krajowe programy certyfikacji o tym samym zakresie powinny zaprzestać wydawania certyfikatów po określonym okresie przejściowym, o którym mowa w art. 57 ust. 1 rozporządzenia (UE) 2019/881.

(27) Krajowe programy certyfikacji powinny polegać na istniejących ramach i w stosownych przypadkach ponownie wykorzystywać dowody w celu zapewnienia harmonizacji i interoperacyjności. Państwa członkowskie mogą zawierać umowy dotyczące transgranicznego ponownego wykorzystania programów certyfikacji lub ich części. Komisja Europejska i ENISA powinny, razem z grupą współpracy, wspierać państwa członkowskie w opracowywaniu i utrzymywaniu ich krajowych programów certyfikacji, zapewniając wymianę wiedzy i najlepsze praktyki.

(28) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([9]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 30 września 2024 r.

(29) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu, o którym mowa w art. 48 ust. 1 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

Niniejsze rozporządzenie określa normy referencyjne oraz ustanawia specyfikacje i procedury w celu stworzenia solidnych ram certyfikacji portfeli, które mają być regularnie aktualizowane w celu zapewnienia zgodności z rozwojem technologii i opracowywanymi normami oraz z pracami prowadzonymi na podstawie zalecenia (UE) 2021/946 w sprawie wspólnego unijnego zestawu narzędzi na potrzeby skoordynowanego podejścia do europejskich ram tożsamości cyfrowej, w szczególności z architekturą i ramami odniesienia.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „rozwiązanie w zakresie portfela" oznacza połączenie oprogramowania, sprzętu, usług, ustawień i konfiguracji, z uwzględnieniem instancji portfela, co najmniej jednej bezpiecznej aplikacji kryptograficznej portfela oraz co najmniej jednego bezpiecznego urządzenia kryptograficznego portfela;

2) „właściciel programu" oznacza organizację odpowiedzialną za opracowanie i utrzymanie programu certyfikacji;

3) „przedmiot certyfikacji" oznacza produkty, procesy i usługi lub ich połączenie, w przypadku których mają zastosowanie określone wymogi;

4) „bezpieczna aplikacja kryptograficzna portfela" oznacza aplikację, która zarządza aktywami krytycznymi, łącząc się z funkcjami kryptograficznymi i niekryptograficznymi zapewnianymi przez bezpieczne urządzenie kryptograficzne portfela oraz korzystając z tych funkcji;

5) „instancja portfela" oznacza aplikację zainstalowaną i skonfigurowaną na urządzeniu lub w środowisku użytkownika portfela, która jest częścią jednostki portfela i z której użytkownik portfela korzysta do interakcji z daną jednostką portfela;

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) „bezpieczne urządzenie kryptograficzne portfela” oznacza urządzenie odporne na manipulacje, które zapewnia otoczenie połączone z bezpieczną aplikacją kryptograficzną portfela i przez nią wykorzystywane, aby chronić aktywa krytyczne i zapewniać funkcje kryptograficzne na potrzeby bezpiecznego wykonywania operacji krytycznych;

7) „rejestr ryzyka” oznacza zapis informacji istotnych z punktu widzenia procesu certyfikacji, dotyczących zidentyfikowanych rodzajów ryzyka;

8) „dostawca portfela” oznacza osobę fizyczną lub prawną, która dostarcza rozwiązania w zakresie portfela;

9) „jednostka certyfikująca” oznacza zewnętrzną jednostkę oceniającą zgodność, która obsługuje programy certyfikacji;

10) „jednostka portfela” oznacza niepowtarzalną konfigurację rozwiązania w zakresie portfela, która obejmuje instancje portfela, bezpieczne aplikacje kryptograficzne portfela i bezpieczne urządzenia kryptograficzne portfela dostarczane przez dostawcę portfela indywidualnemu użytkownikowi portfela;

11) „aktywa krytyczne” oznaczają aktywa wewnątrz jednostki portfela lub z nią związane o tak istotnym znaczeniu, że naruszenie ich dostępności, poufności lub integralności miałoby bardzo poważny, szkodliwy wpływ na zdolność do polegania na danej jednostce portfela;

12) „użytkownik portfela” oznacza użytkownika, który kontroluje jednostkę portfela;

13) „incydent” oznacza incydent zgodnie z definicją w art. 6 pkt 6 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 ([10]);

14) „wbudowane reguły ujawniania” oznaczają zbiór zasad wbudowanych w elektronicznym poświadczeniu atrybutów przez dostawcę tego poświadczenia; zasady te określają warunki, jakie musi spełnić strona ufająca portfela, aby uzyskać dostęp do elektronicznego poświadczenia atrybutów.

ROZDZIAŁ II

KRAJOWE PROGRAMY CERTYFIKACJI

Artykuł 3

Ustanowienie krajowych programów certyfikacji

1. Państwa członkowskie wyznaczają właściciela programu w odniesieniu do każdego krajowego programu certyfikacji.

2. Celem certyfikacji określonym w krajowych programach certyfikacji jest zapewnianie i obsługa rozwiązań w zakresie portfela oraz systemów identyfikacji elektronicznej, w ramach których są one zapewniane.

3. Zgodnie z rozporządzeniem wykonawczym (UE) 2015/1502 przedmiot certyfikacji w ramach krajowych programów certyfikacji obejmuje następujące elementy:

a) komponenty oprogramowania, w tym ustawienia i konfiguracje rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są zapewniane rozwiązania w zakresie portfela;

b) komponenty sprzętu oraz platformy, na których działają lub na których opierają się komponenty oprogramowania, o których mowa w pkt b), w przypadkach, gdy są one zapewniane bezpośrednio lub pośrednio przez rozwiązanie w zakresie portfela oraz system identyfikacji elektronicznej, w ramach którego są one zapewniane, i gdy są wymagane do osiągnięcia pożądanego poziomu pewności dla tych komponentów oprogramowania. Jeżeli komponenty sprzętu oraz platformy nie są dostarczane przez dostawcę portfela, krajowe programy certyfikacji powinny sformułować założenia dla oceny komponentów sprzętu komputerowego i platform, w ramach których można zapewnić odporność na atakujących dysponujących wysokim potencjałem ataku zgodnie z rozporządzeniem wykonawczym (UE) 2015/1502, oraz określić działania w zakresie oceny w celu potwierdzenia tych założeń, o których mowa w załączniku IV;

([10]) 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) procesy wspierające zapewnianie i obsługę rozwiązania w zakresie portfela, w tym proces rejestracji użytkownika, o którym mowa w art. 5a rozporządzenia (UE) nr 910/2014, obejmujące co najmniej wprowadzenie do systemu, zarządzanie środkami elektronicznymi i organizację zgodnie z sekcjami 2.1, 2.2 i 2.4 załącznika I do rozporządzenia wykonawczego (UE) 2015/1502.

4. Krajowe programy certyfikacji muszą zawierać opis konkretnej architektury rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane. W przypadku gdy krajowe programy certyfikacji obejmują więcej niż jedną konkretną architekturę, powinny zawierać profil dla każdej z tych architektur.

5. W odniesieniu do każdego profilu krajowe programy certyfikacji muszą określać co najmniej następujące elementy:

a) specyficzną architekturę rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane;

b) kontrole bezpieczeństwa związane z poziomami bezpieczeństwa określonymi w art. 8 rozporządzenia (UE) nr 910/2014;

c) plan oceny sporządzony zgodnie z pkt 7.4.1 normy EN ISO/IEC 17065:2012;

d) wymogi bezpieczeństwa niezbędne do przeciwdziałania ryzyku w cyberprzestrzeni i zagrożeniom cyberbezpieczeństwa wymienionym w rejestrze ryzyka określonym w załączniku I do niniejszego rozporządzenia, do wymaganego poziomu bezpieczeństwa, oraz – w stosownych przypadkach – do osiągnięcia celów określonych w art. 51 rozporządzenia (UE) 2019/881;

e) przyporządkowania kontroli, o których mowa w lit. b) niniejszego ustępu, do komponentów architektury;

f) opis sposobu, w jaki kontrole bezpieczeństwa, przyporządkowywanie, wymogi bezpieczeństwa i plan oceny, o których mowa w lit. b)–c), umożliwiają dostawcom rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, odpowiednie przeciwdziałanie ryzyku w cyberprzestrzeni i zagrożeniom cyberbezpieczeństwa zidentyfikowanym w rejestrze ryzyka, o którym mowa w lit. d), do wymaganego poziomu bezpieczeństwa określonego w oparciu o ocenę ryzyka, aby doprecyzować i uzupełnić ryzyka i zagrożenia ujęte w rejestrze ryzyka o ryzyka i zagrożenia specyficzne dla danej architektury.

6. Plan oceny, o którym mowa w ust. 5 lit. c), zawiera wykaz działań w zakresie oceny, które należy uwzględnić w ocenie rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane.

7. W ramach działań w zakresie oceny, o których mowa w ust. 6, wymaga się od dostawców rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, przekazania informacji spełniających wymogi wymienione w załączniku II.

Artykuł 4

Wymogi ogólne

1. Krajowe programy certyfikacji obejmują wymogi funkcjonalne oraz wymogi związane z cyberbezpieczeństwem i ochroną danych, wykorzystując, w miarę dostępności i w stosownych przypadkach, następujące programy certyfikacji:

a) europejskie programy certyfikacji cyberbezpieczeństwa ustanowione na podstawie rozporządzenia (UE) 2019/881, w tym EUCC;

b) krajowe programy certyfikacji cyberbezpieczeństwa objęte EUCC zgodnie z art. 49 rozporządzenia wykonawczego (UE) 2024/482.

2. Krajowe programy certyfikacji mogą dodatkowo, w miarę dostępności i w stosownych przypadkach, odnosić się do:

a) innych odpowiednich krajowych programów certyfikacji;

b) norm międzynarodowych, europejskich i krajowych;

c) specyfikacji technicznych spełniających wymogi określone w załączniku II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 ([11]).

3. Krajowe programy certyfikacji:

a) określają elementy wymienione w pkt 6.5 normy EN ISO/IEC 17067:2013;

b) są wdrażane jako program typu 6 zgodnie z pkt 5.3.8 normy EN ISO/IEC 17067:2013.

4. Krajowe programy certyfikacji muszą spełniać następujące wymagania:

a) tylko dostawcy wymienieni w art. 5a ust. 2 rozporządzenia (UE) nr 910/2014 są uprawnieni do otrzymania certyfikatów w ramach krajowych programów certyfikacji;

b) jako znaku zgodności używa się wyłącznie znaku zaufania;

c) dostawcy rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, zawierają odniesienia do rozporządzenia (UE) nr 910/2014 i niniejszego rozporządzenia w kontekście programu;

d) dostawcy rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, uzupełniają ocenę ryzyka programu, o której mowa w art. 3 ust. 5 lit. f), w celu zidentyfikowania ryzyk i zagrożeń właściwych dla ich wdrożenia oraz proponują odpowiednie środki zaradcze w odniesieniu do wszystkich istotnych rodzajów ryzyka i zagrożeń;

e) zakres odpowiedzialności oraz działania prawne są ustalane wraz z odniesieniami do obowiązujących przepisów krajowych, które określają zakres odpowiedzialności oraz możliwe działania prawne, w przypadku gdy certyfikacja w ramach systemu jest wykorzystywana w sposób niezgodny z przepisami.

5. Ocenę, o której mowa w ust. 4 lit. d), udostępnia się jednostce certyfikującej do celów ewaluacji.

Artykuł 5

Zarządzanie incydentami i podatnościami na zagrożenia

1. Krajowe programy certyfikacji zawierają wymogi w zakresie zarządzania incydentami i podatnościami na zagrożenia zgodnie z ust. 2–9.

2. Posiadacz certyfikatu zgodności rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, niezwłocznie notyfikuje swojej jednostce certyfikującej wszelkie przypadki naruszenia bezpieczeństwa lub kompromitacji rozwiązania w zakresie portfela lub systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, mogących wpłynąć na jego zgodność z wymogami krajowych programów certyfikacji.

3. Posiadacz certyfikatu zgodności ustanawia, utrzymuje i stosuje politykę i procedury zarządzania podatnościami na zagrożenia, z uwzględnieniem procedur określonych w istniejących normach europejskich i międzynarodowych, w tym w normie EN ISO/IEC 30111:2019.

4. Posiadacz certyfikatu zgodności notyfikuje jednostkę certyfikującą, która go wydała, o podatnościach na zagrożenia i zmianach mających wpływ na rozwiązanie w zakresie portfela, w oparciu o określone kryteria dotyczące wpływu tych podatności i zmian.

5. Posiadacz certyfikatu zgodności przygotowuje sprawozdanie z analizy skutków podatności na zagrożenia w odniesieniu do każdej podatności na zagrożenia, która ma wpływ na komponenty oprogramowania rozwiązania w zakresie portfela. Sprawozdanie musi zawierać następujące informacje:

a) wpływ podatności na zagrożenia na certyfikowane rozwiązanie w zakresie portfela;

b) możliwe zagrożenia związane z nadchodzącym lub potencjalnym atakiem;

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) czy podatność na zagrożenia może zostać wyeliminowana za pomocą dostępnych środków;

d) w przypadku gdy podatność na zagrożenia może zostać wyeliminowana za pomocą dostępnych środków – możliwe sposoby jej wyeliminowania.

6. W przypadku gdy notyfikacja jest wymagana zgodnie z ust. 4, posiadacz certyfikatu zgodności niezwłocznie przekazuje jednostce certyfikującej sprawozdanie z analizy skutków podatności na zagrożenia, o którym mowa w ust. 5.

7. Posiadacz certyfikatu zgodności ustanawia, utrzymuje i prowadzi politykę zarządzania podatnościami na zagrożenia spełniającą wymogi określone w załączniku I do aktu dotyczącego cyberodporności ([12]).

8. Krajowe programy certyfikacji ustanawiają wymogi dotyczące ujawniania podatności na zagrożenia mające zastosowanie do jednostek certyfikujących.

9. Posiadacz certyfikatu zgodności musi ujawniać i rejestrować wszelkie publicznie znane i wyeliminowane podatności na zagrożenia w rozwiązaniu w zakresie portfela lub w jednym z internetowych repozytoriów, o których mowa w załączniku V.

Artykuł 6

Utrzymywanie krajowych programów certyfikacji

1. Krajowe programy certyfikacji obejmują procedurę okresowego przeglądu działalności. Procedura ta ma na celu potwierdzenie ich adekwatności i określenie aspektów wymagających poprawy, z uwzględnieniem informacji zwrotnych od zainteresowanych stron.

2. Krajowe programy certyfikacji zawierają przepisy dotyczące ich utrzymania. Procedura ta musi obejmować co najmniej następujące wymogi:

a) zasady zarządzania definicjami i wymogami krajowych programów certyfikacji;

b) ustanowienie terminów wydawania świadectw po przyjęciu zaktualizowanych wersji krajowych programów certyfikacji, zarówno w odniesieniu do nowych, jak i wydanych wcześniej certyfikatów zgodności;

c) okresowy przegląd krajowych programów certyfikacji w celu zapewnienia spójnego stosowania wymogów krajowych programów certyfikacji, z uwzględnieniem co najmniej następujących elementów:

— wnioski o wyjaśnienie skierowane do właściciela programu w odniesieniu do wymogów krajowego programu certyfikacji;

— informacje zwrotne od zainteresowanych stron i innych interesariuszy;

— zdolność właściciela krajowego programu certyfikacji do reagowania na wnioski o udzielenie informacji;

d) zasady monitorowania dokumentów referencyjnych i procedur rozwoju wersji referencyjnych krajowych programów certyfikacji, z uwzględnieniem co najmniej okresów przejściowych;

e) procedura zapewniająca uwzględnienie najnowszych ryzyk w cyberprzestrzeni i zagrożeń cyberbezpieczeństwa wymienionych w rejestrze ryzyka określonym w załączniku I do niniejszego rozporządzenia;

f) proces zarządzania pozostałymi zmianami w krajowych programach certyfikacji.

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz.U. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Krajowe programy certyfikacji zawierają wymogi dotyczące przeprowadzania ocen obecnie certyfikowanych produktów we wskazanym okresie po zmianie programu lub po opublikowaniu nowych specyfikacji lub norm, lub ich nowych wersji, z którymi muszą być zgodne rozwiązania w zakresie portfela oraz system identyfikacji elektronicznej, w ramach którego są one zapewniane.

ROZDZIAŁ III

WYMOGI DOTYCZĄCE WŁAŚCICIELI PROGRAMÓW

Artykuł 7

Wymogi ogólne

1. Właściciele programów opracowują i utrzymują krajowe programy certyfikacji oraz regulują ich działalność.

2. Właściciele programów mogą zlecić podwykonawstwo całości lub części swoich zadań osobie trzeciej. Zlecając podwykonawstwo podmiotowi prywatnemu, właściciele programów określają obowiązki i zakres odpowiedzialności wszystkich stron w drodze umowy. Właściciele programów ponoszą odpowiedzialność za wszystkie zlecone podwykonawcom czynności wykonywane przez ich podwykonawców.

3. Właściciele programów prowadzą działania monitorujące, w stosownych przypadkach, wykorzystując do tego celu co najmniej następujące informacje:

a) informacje pochodzące od jednostek certyfikujących, krajowych jednostek akredytujących i odpowiednich organów nadzoru rynku;

b) informacje uzyskane w wyniku kontroli i dochodzeń prowadzonych przez właścicieli systemów lub przez inne organy;

c) skargi i odwołania otrzymane na podstawie art. 15.

4. Właściciele programów informują grupę współpracy o zmianach krajowych programów certyfikacji. Notyfikacja taka musi zawierać odpowiednie informacje umożliwiające grupie współpracy wydawanie zaleceń dla właścicieli programów oraz opinii na temat zaktualizowanych krajowych programów certyfikacji.

ROZDZIAŁ IV

WYMOGI DOTYCZĄCE DOSTAWCÓW ROZWIĄZAŃ W ZAKRESIE PORTFELA ORAZ SYSTEMU IDENTYFIKACJI ELEKTRONICZNEJ, W RAMACH KTÓREGO SĄ ONE ZAPEWNIANE

Artykuł 8

Wymogi ogólne

1. Krajowe programy certyfikacji zawierają wymogi związane z cyberbezpieczeństwem oparte na ocenie ryzyka każdej konkretnej obsługiwanej architektury. Wymogi związane z cyberbezpieczeństwem mają na celu traktowanie zidentyfikowanych ryzyk w cyberprzestrzeni i zagrożeń cyberbezpieczeństwa zgodnie z rejestrem ryzyka określonym w załączniku I.

2. Zgodnie z art. 5a ust. 23 rozporządzenia (UE) nr 910/2014 krajowe programy certyfikacji wymagają, aby rozwiązania w zakresie portfela oraz systemy identyfikacji elektronicznej, w ramach których są one zapewniane, były odporne na atakujących dysponujących wysokim potencjałem ataku w przypadku wysokiego poziomu bezpieczeństwa, o których mowa w rozporządzeniu wykonawczym (UE) 2015/1502.

3. W krajowych programach certyfikacji należy ustanowić kryteria bezpieczeństwa, które obejmują następujące wymogi:

a) akt o cyberodporności, w stosownych przypadkach, lub wymogi spełniające cele bezpieczeństwa określone w art. 51 rozporządzenia (UE) 2019/881;

b) ustanowienie i wdrożenie polityk i procedur dotyczących zarządzania ryzykiem związanym z obsługą rozwiązania w zakresie portfela, w tym identyfikacji i oceny ryzyka oraz ograniczania zidentyfikowanego ryzyka;

c) ustanowienie i wdrożenie polityk i procedur związanych z zarządzaniem zmianą i zarządzaniem podatnościami zgodnie z art. 5 niniejszego rozporządzenia;

d) ustanowienie i wdrożenie polityk i procedur w zakresie zarządzania zasobami ludzkimi, z uwzględnieniem wymogów dotyczących wiedzy fachowej, wiarygodności, doświadczenia, szkoleń w zakresie bezpieczeństwa oraz kwalifikacji personelu zaangażowanego w opracowywanie lub obsługę rozwiązania w zakresie portfela;

e) wymogi dotyczące środowiska operacyjnego rozwiązania w zakresie portfela, również w formie założeń dotyczących bezpieczeństwa urządzeń i platform, na których działają komponenty oprogramowania rozwiązania w zakresie portfela, łącznie z WSCD oraz, w stosownych przypadkach, wymogi dotyczące oceny zgodności w celu potwierdzenia, że założenia te są weryfikowane na odpowiednich urządzeniach i platformach;

f) w odniesieniu do każdego założenia, które nie jest potwierdzone certyfikatem zgodności lub innymi akceptowalnymi informacjami na temat bezpieczeństwa – opis mechanizmu wykorzystywanego przez dostawcę portfela w celu wyegzekwowania założenia, a także uzasadnienie, że mechanizm ten jest wystarczający do zapewnienia weryfikacji tego założenia;

g) ustanowienie i wdrożenie środków zapewniających wykorzystanie aktualnie certyfikowanej wersji rozwiązania w zakresie portfela.

4. Krajowe programy certyfikacji zawierają wymogi funkcjonalne dotyczące mechanizmów aktualizacji dla każdego komponentu oprogramowania rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach których są one zapewniane, dla operacji wymienionych w załączniku III.

5. Krajowe programy certyfikacji wymagają, aby podmiot ubiegający się o certyfikację dostarczył lub w inny sposób udostępnił jednostce certyfikującej następujące informacje i dokumentację:

a) dowody dotyczące informacji, o których mowa w załączniku IV pkt 1, z uwzględnieniem, w razie potrzeby, szczegółowych informacji na temat rozwiązania w zakresie portfela i jego kodu źródłowego, w tym:

— *informacje dotyczące architektury*: w odniesieniu do każdego komponentu rozwiązania w zakresie portfela (w tym komponentów produktu, procesu i usługi) – opis jego podstawowych cech bezpieczeństwa, w tym zależności zewnętrznych;

— *kontrole i poziomy bezpieczeństwa*: w odniesieniu do każdej kontroli bezpieczeństwa rozwiązania w zakresie portfela – opis kontroli i wymaganego poziomu bezpieczeństwa na podstawie załącznika do rozporządzenia wykonawczego (UE) 2015/1502, w którym określono szereg specyfikacji technicznych i procedur mających zastosowanie do poszczególnych kontroli wdrażanych za pomocą środków identyfikacji elektronicznej;

— *przyporządkowanie kontroli do komponentów architektury*: opis sposobu, w jaki kontrole portfela są wdrażane z wykorzystaniem poszczególnych komponentów rozwiązania w zakresie portfela, w oparciu o podstawy wyjaśniające, dlaczego wymagany jest dany poziom bezpieczeństwa, oraz w jaki sposób kontrola jest realizowana z uwzględnieniem wszystkich wymaganych aspektów bezpieczeństwa na odpowiednim poziomie;

— *podstawy i uzasadnienie dotyczące zabezpieczenia przed ryzykiem*: uzasadnienie:

— przyporządkowania kontroli do komponentów;

— adekwatności proponowanego planu oceny do odpowiedniego uwzględnienia wszystkich kontroli;

— zakresu kontroli ryzyk w cyberprzestrzeni i zagrożeń cyberbezpieczeństwa zidentyfikowanych w rejestrze ryzyka, uzupełnionych kontrolami ryzyka i zagrożeń właściwych dla wdrożenia, na odpowiednim poziomie bezpieczeństwa;

b) informacje wymienione w załączniku V;

c) pełen wykaz certyfikatów zgodności i innych informacji na temat bezpieczeństwa wykorzystywanych jako dowody w trakcie działań w zakresie oceny;

d) wszelkie inne informacje istotne na potrzeby działań w zakresie oceny.

ROZDZIAŁ V

WYMOGI DOTYCZĄCE JEDNOSTEK CERTYFIKUJĄCYCH

Artykuł 9

Wymogi ogólne

1. Jednostki certyfikujące są akredytowane przez krajowe jednostki akredytujące wyznaczone na podstawie rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 ([13]), zgodnie z normą EN ISO/IEC 17065:2012, pod warunkiem że spełniają one wymogi określone w krajowych programach certyfikacji zgodnie z ust. 2.

2. Do celów akredytacji jednostki certyfikujące muszą spełnić wszystkie następujące wymogi w zakresie kompetencji:

a) posiadać szczegółową i techniczną wiedzę na temat odpowiedniej architektury rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, jak również na temat zagrożeń i ryzyka związanych z tymi architekturami;

b) wykazać się znajomością dostępnych rozwiązań w zakresie bezpieczeństwa i ich właściwości zgodnie z załącznikiem do rozporządzenia wykonawczego (UE) 2015/1502;

c) wykazać się znajomością czynności wykonywanych na podstawie certyfikatów zgodności stosowanych do komponentów rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, jako przedmiot certyfikacji;

d) posiadać szczegółową wiedzę na temat mającego zastosowanie krajowego programu certyfikacji ustanowionego zgodnie z rozdziałem II.

3. Jednostki certyfikujące mają obowiązek wykonywać swoje działania w zakresie nadzoru, wykorzystując do tego celu w szczególności następujące informacje:

a) informacje pochodzące od krajowych jednostek akredytujących i odpowiednich organów nadzoru rynku;

b) informacje wynikające z kontroli i dochodzeń prowadzonych przez jednostki certyfikujące lub przez inne organy;

c) skargi i odwołania otrzymane na podstawie art. 15.

Artykuł 10

Podwykonawstwo

Jednostki certyfikujące mogą zlecić stronom trzecim podwykonawstwo działań w zakresie oceny, o których mowa w art. 13. W przypadku zlecania podwykonawcom działań w zakresie oceny krajowe programy certyfikacji ustalają co następuje:

1) wszyscy podwykonawcy jednostki certyfikującej przeprowadzający działania w zakresie oceny – gdy jest to konieczne do celów działań, które mają być wykonane – mają obowiązek spełniać wymogi norm zharmonizowanych, takich jak EN ISO/IEC 17025:2017 w odniesieniu do badań, EN ISO/IEC 17020:2012 w odniesieniu do kontroli, EN ISO/IEC 17021-1:2015 w odniesieniu do kontroli i EN ISO/IEC 17029:2019 w odniesieniu do walidacji i weryfikacji;

2) jednostki certyfikujące ponoszą odpowiedzialność za wszystkie działania w zakresie oceny zlecone innym podmiotom i wykazują, że wprowadziły odpowiednie środki w trakcie akredytacji, w tym, w stosownych przypadkach, opierając się na własnej akredytacji swoich podwykonawców;

3) stopień, w jakim uprzednia zgoda na outsourcing jest uzyskiwana od właścicieli programów lub klienta, którego rozwiązanie w zakresie portfela jest certyfikowane w ramach programu certyfikacji.

([13]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Artykuł 11

Notyfikowanie organu nadzoru

Jednostki certyfikujące notyfikują organ nadzoru, o którym mowa w art. 46a ust. 1 rozporządzenia (UE) nr 910/2014, o wydaniu, zawieszeniu i odwołaniu certyfikatów zgodności rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane.

Artykuł 12

Zarządzanie incydentami i podatnościami na zagrożenia

1. Jednostki certyfikujące bez zbędnej zwłoki zawieszają certyfikat zgodności rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego jest ono zapewniane, po potwierdzeniu przez te jednostki, że notyfikowane naruszenie lub kompromitacja bezpieczeństwa mają wpływ na zgodność z wymaganiami krajowych programów certyfikacji rozwiązania w zakresie portfela lub systemu identyfikacji elektronicznej, w ramach którego są one zapewniane.

2. Jednostki certyfikujące odwołują certyfikat zgodności, który został zawieszony w wyniku naruszenia lub zagrożenia bezpieczeństwa, których nie wyeliminowano w odpowiednim czasie.

3. Jednostki certyfikujące odwołują certyfikaty zgodności, jeżeli nie zaradzono zidentyfikowanej podatności na zagrożenia w odpowiednim czasie proporcjonalnie do jej wagi i potencjalnego wpływu, zgodnie z art. 5c ust. 4 i art. 5e ust. 2 rozporządzenia (UE) nr 910/2014.

ROZDZIAŁ VI

CZYNNOŚCI Z ZAKRESU OCENY ZGODNOŚCI

Artykuł 13

Działania w zakresie oceny

1. Krajowe programy certyfikacji zawierają metody i procedury, które mają być stosowane przez jednostki oceniające zgodność podczas prowadzenia działań w zakresie oceny zgodnie z normą EN ISO/IEC 17065:2012, uwzględniające co najmniej następujące elementy:

a) metody i procedury prowadzenia działań w zakresie oceny, w tym te związane z WSCD, jak określono w załączniku IV;

b) kontrolę wdrożenia rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, w oparciu o rejestr ryzyka określony w załączniku I i uzupełniony, w razie potrzeby, o ryzyko charakterystyczne dla procesu wdrożenia;

c) działania w zakresie testowania funkcjonalnego, oparte, o ile są dostępne i stosowne, na zestawach testów, które są zdefiniowane zgodnie ze specyfikacjami technicznymi lub normami;

d) ocenę istnienia i przydatności procesów utrzymania, w tym co najmniej zarządzania wersjami, zarządzania aktualizacjami i zarządzania podatnościami na zagrożenia;

e) ocenę skuteczności operacyjnej procesów utrzymania, w tym co najmniej zarządzanie wersjami, zarządzanie aktualizacjami i zarządzanie podatnościami na zagrożenia;

f) analizę zależności przedstawioną przez dostawcę portfela, w tym metodykę oceny dopuszczalności informacji na temat bezpieczeństwa, która obejmuje elementy określone w załączniku VI;

g) ocenę podatności na zagrożenia, na odpowiednim poziomie, z uwzględnieniem:

— przeglądu projektu rozwiązania w zakresie portfela oraz, w stosownych przypadkach, jego kodu źródłowego;

— badania odporności rozwiązania w zakresie portfela na atakujących dysponujących wysokim potencjałem ataku przy wysokim poziomie bezpieczeństwa zgodnie z sekcją 2.2.1 załącznika do rozporządzenia wykonawczego (UE) 2015/1502;

h) ocena rozwoju środowiska zagrożenia i jego wpływu na uwzględnienie ryzyka w rozwiązaniu w zakresie portfela w celu określenia, jakie działania w zakresie oceny są wymagane w odniesieniu do poszczególnych komponentów rozwiązania w zakresie portfela.

2. Krajowe programy certyfikacji zawierają ocenę mającą na celu ustalenie, czy wdrożenie rozwiązań w zakresie portfela i systemu identyfikacji elektronicznej, w ramach których te rozwiązania w zakresie portfela są zapewniane, są zgodne z architekturą określoną w art. 3 ust. 5 lit. a), jak również ocenę mającą na celu ustalenie, czy plan oceny zaproponowany wraz z wdrożeniem jest zgodny z planem oceny, o którym mowa w art. 3 ust. 5 lit. c).

3. Krajowe programy certyfikacji określają zasady doboru próby, aby uniknąć powtarzania identycznych działań w zakresie oceny i skoncentrować się na działaniach, które są specyficzne dla danego wariantu. Takie zasady doboru próby umożliwiają przeprowadzanie badań funkcjonalnych i badań bezpieczeństwa wyłącznie na próbce wariantów komponentu docelowego rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego jest one zapewniane, oraz na próbce urządzeń docelowych. Krajowe programy certyfikacji wymagają od wszystkich jednostek certyfikujących uzasadnienia stosowania przez nie doboru próby.

4. Krajowe programy certyfikacji wymagają przeprowadzenia przez jednostkę certyfikującą oceny WSCA w oparciu o metody i procedury określone w załączniku IV.

Artykuł 14

Działania w zakresie certyfikacji

1. Krajowe programy certyfikacji określają działanie w zakresie poświadczenia do celów wydania certyfikatu zgodności, zgodnie z sekcją V lit. a) tabela 1 normy EN ISO/IEC 17067:2013, w tym następujące elementy:

a) treść certyfikatu zgodności, jak określono w załączniku VII;

b) sposób przedstawiania wyników oceny w ogólnodostępnym raporcie z certyfikacji, w tym co najmniej streszczenia wstępnego planu kontroli i planu walidacji, jak określono w załączniku VIII;

c) treść wyników oceny przedstawionych w sprawozdaniu z oceny certyfikacji, w tym elementy określone w załączniku VIII.

2. Sprawozdanie z oceny certyfikacji może zostać udostępnione grupie współpracy i Komisji.

Artykuł 15

Skargi i odwołania

Krajowe programy certyfikacji zawierają procedury lub odniesienia do mających zastosowanie przepisów krajowych, określających mechanizm skutecznego składania i rozpatrywania skarg i odwołań w związku z wdrażaniem przez nie programu certyfikacji lub wydanego certyfikatu zgodności. Procedury te obejmują przekazywanie skarżącemu informacji o przebiegu postępowania oraz o podjętej decyzji, a także informowanie skarżącego o prawie do skutecznego środka prawnego przed sądem. Krajowe programy certyfikacji wymagają, aby wszystkie skargi i odwołania, które nie zostały lub nie mogą zostać rozstrzygnięte przez jednostkę certyfikującą, były przesyłane właścicielowi programu w celu dokonania oceny i rozstrzygnięcia.

Artykuł 16

Działania w zakresie nadzoru

1. Krajowe programy certyfikacji wymagają od jednostek certyfikujących wdrożenia działań w zakresie nadzoru obejmujących ocenę nadzoru nad procesami połączoną z badaniami wyrywkowymi lub inspekcjami.

2. Krajowe programy certyfikacji zawierają, w stosownych przypadkach, wymogi dla właścicieli programów w zakresie monitorowania zgodności jednostek certyfikujących z ich obowiązkami zgodnie z rozporządzeniem (UE) nr 910/2014 i krajowymi programami certyfikacji.

3. Krajowe programy certyfikacji zawierają wymogi, przy pomocy których jednostki certyfikujące monitorują:

a) wypełnianie przez posiadaczy certyfikatu zgodności wydanego w ramach krajowych programów certyfikacji ich obowiązków w zakresie certyfikacji na podstawie rozporządzenia (UE) nr 910/2014 i krajowych programów certyfikacji;

b) zgodność certyfikowanego rozwiązania w zakresie portfela z wymogami określonymi w krajowych programach certyfikacji.

Artykuł 17

Konsekwencje niezgodności

Krajowe programy certyfikacji określają konsekwencje niezgodności certyfikowanego rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, z wymogami określonymi w niniejszym rozporządzeniu. Konsekwencje te obejmują następujące elementy:

1) spoczywający na jednostce certyfikującej obowiązek poinformowania posiadacza certyfikatu zgodności oraz żądania podjęcia działań naprawczych przez tego posiadacza certyfikatu zgodności;

2) spoczywający na jednostce certyfikującej obowiązek informowania innych właściwych organów nadzoru rynku, jeżeli niezgodność dotyczy odpowiednich przepisów Unii;

3) warunki przeprowadzania działań naprawczych przez posiadacza certyfikatu zgodności;

4) warunki zawieszenia certyfikatu zgodności przez jednostkę certyfikującą i przywrócenia certyfikatu zgodności po usunięciu niezgodności;

5) warunki odwołania certyfikatu zgodności przez jednostkę certyfikującą;

6) konsekwencje nieprzestrzegania przez jednostkę certyfikującą wymogów krajowego programu certyfikacji.

ROZDZIAŁ VII

CYKL ŻYCIA CERTYFIKACJI

Artykuł 18

Cykl życia certyfikacji

1. Jednostka certyfikująca prowadzi regularne działania w zakresie oceny ważności certyfikatów zgodności wydanych w ramach krajowych programów certyfikacji zgodnie z wymogami określonymi w załączniku IX.

2. Krajowe programy certyfikacji zawierają procedurę ponownej certyfikacji rozwiązań w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, na żądanie posiadacza certyfikatu zgodności przed wygaśnięciem pierwotnego certyfikatu zgodności. Procedura ponownej certyfikacji obejmuje pełną ocenę rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, w tym ocenę podatności, zgodnie z zasadami określonymi w załączniku IX.

3. Krajowe programy certyfikacji obejmują proces zarządzania zmianami w certyfikowanym rozwiązaniu w zakresie portfela oraz systemie identyfikacji elektronicznej, w ramach którego są one zapewniane. Procedura ta obejmuje zasady ustalania, czy zmiana ma zostać objęta specjalną oceną, o której mowa w ust. 4, lub weryfikacją skuteczności operacyjnej procesów utrzymania, o której mowa w załączniku IV.

4. Krajowe programy certyfikacji uwzględniają procedurę dotyczącą specjalnych ocen zgodnie z normą EN ISO/IEC 17065:2012. Proces specjalnych ocen obejmuje wybór czynności, które należy przeprowadzić w celu rozwiązania konkretnego problemu, który doprowadził do przeprowadzenia specjalnej oceny.

5. Krajowe programy certyfikacji określają zasady dotyczące odwołania certyfikatu zgodności.

ROZDZIAŁ VIII

PROWADZENIE REJESTRÓW I OCHRONA INFORMACJI

Artykuł 19

Przechowywanie wpisów

1. Krajowe programy certyfikacji zawierają wymogi dla jednostek certyfikujących dotyczące systemu wpisów zawierającego wszystkie istotne informacje uzyskane w związku z prowadzonymi przez nie czynnościami z zakresu oceny zgodności, w tym dane wydane i otrzymane przez dostawców rozwiązań w zakresie portfela oraz systemów identyfikacji elektronicznej, w ramach których są one zapewniane. Wpisy zawierające takie informacje przechowuje się w sposób bezpieczny. Wpisy mogą być przechowywane w formie elektronicznej i pozostawać dostępne tak długo, jak wymaga tego prawo Unii lub prawo krajowe oraz przez okres co najmniej pięciu lat po odwołaniu lub wygaśnięciu odpowiedniego certyfikatu zgodności.

2. Krajowe programy certyfikacji określają wymogi, zgodnie z którymi posiadacz certyfikatu zgodności musi bezpiecznie przechowywać następujące informacje do celów niniejszego rozporządzenia i przez okres co najmniej pięciu lat po odwołaniu lub wygaśnięciu odpowiedniego certyfikatu zgodności:

a) wpisy zawierające informacje przekazane jednostce certyfikującej lub jej podwykonawcom w trakcie procesu certyfikacji;

b) wzory komponentów sprzętu, które zostały objęte zakresem certyfikacji dla rozwiązania w zakresie portfela.

3. Krajowe programy certyfikacji wymagają, aby posiadacz certyfikatu zgodności udostępniał na żądanie jednostki certyfikującej lub organu nadzoru, o którym mowa w art. 46a ust. 1 rozporządzenia (UE) nr 910/2014, informacje, o których mowa w ust. 1.

Artykuł 20

Ochrona informacji

W ramach krajowych programów certyfikacji wszystkie osoby lub organizacje, którym przyznano dostęp do informacji podczas wykonywania działań w ramach krajowego programu certyfikacji, są zobowiązane do zapewnienia bezpieczeństwa i ochrony tajemnic handlowych oraz innych informacji poufnych oraz zachowania praw własności intelektualnej, a także do wprowadzenia niezbędnych i odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poufności takich danych.

ROZDZIAŁ IX

PRZEPISY KOŃCOWE

Artykuł 21

Przejście na europejski program certyfikacji cyberbezpieczeństwa

Niniejsze rozporządzenie podlega przeglądowi w momencie przyjęcia pierwszego europejskiego programu certyfikacji cyberbezpieczeństwa rozwiązań w zakresie portfela oraz systemów identyfikacji elektronicznej, w ramach których są one zapewniane, w celu uwzględnienia wkładu takiego europejskiego programu certyfikacji cyberbezpieczeństwa w ogólną certyfikację rozwiązań w zakresie portfela oraz systemów identyfikacji elektronicznej, w ramach których są one zapewniane.

Artykuł 22

Wejście w życie

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

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

Sporządzono w Brukseli dnia 28 listopada 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

REJESTR RYZYKA EUROPEJSKICH PORTFELI TOŻSAMOŚCI CYFROWEJ

Wprowadzenie

Rejestr ryzyka opisuje główne rodzaje ryzyka i zagrożeń związane z bezpieczeństwem i prywatnością, które dotyczą portfeli i które należy odpowiednio uwzględnić w każdej architekturze i przy wdrażaniu portfeli. **Wysokie ryzyko** (sekcja I) wiąże się z korzystaniem z portfeli przez użytkowników i strony ufające, a także ma związek z bezpośrednimi zagrożeniami wobec aktywów portfeli. Ponadto zidentyfikowano kilka rodzajów **ryzyka na poziomie systemowym** (sekcja II) dla portfeli, zazwyczaj będących skutkiem połączenia zagrożeń mających zastosowanie do całego systemu portfeli.

Rodzaj ryzyka	Identyfikator ryzyka	Powiązane rodzaje ryzyka
Wysokie ryzyko dla portfeli	R1	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej
	R2	Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej
	R3	Tworzenie lub wykorzystywanie fałszywych atrybutów
	R4	Kradzież tożsamości
	R5	Kradzież danych
	R6	Ujawnienie danych
	R7	Manipulacja danymi
	R8	Utrata danych
	R9	Nieupoważniona transakcja
	R10	Manipulacja transakcją
	R11	Zaprzeczenie
	R12	Ujawnienie danych dotyczących transakcji
	R13	Zakłócenie usługi
	R14	Inwigilacja
Ryzyko systemowe	SR1	Inwigilacja hurtowa
	SR2	Nadszarpnięcie reputacji
	SR3	Niezgodność z przepisami prawa

W rejestrze wyróżnia się również **zagrożenia techniczne** (sekcja III) związane z wdrażaniem rozwiązania w zakresie portfela. Zagrożenia te są związane z wysokim ryzykiem, ponieważ każde z nich może zostać wykorzystane do wywoływania wielu rodzajów wysokiego ryzyka.

Rodzaj zagrożenia	Identyfikator zagrożenia	Powiązane zagrożenia	Podkategorie zagrożeń
Zagrożenie techniczne	TT1	Ataki fizyczne	1.1. *Kradzież*
			1.2. *Wyciek informacji*
			1.3. *Ingerencja*
	TT2	Błędy i błędna konfiguracja	2.1. *Błędy podczas zarządzania systemem informatycznym*
			2.2. *Błędy na poziomie aplikacji lub błędy użytkowania*
			2.3. *Błędy na etapie rozwoju i błędne konfiguracje systemu*

Rodzaj zagrożenia	Identyfikator zagrożenia	Powiązane zagrożenia	Podkategorie zagrożeń
	TT3	Korzystanie z niewiarygodnych zasobów	3.1. *Błędne wykorzystanie lub błędna konfiguracja komponentów portfela*
	TT4	Awarie i przestoje	4.1. *Awaria lub dysfunkcja sprzętu, urządzeń lub systemów*
			4.2. *Utrata zasobów*
			4.3. *Utrata usług wsparcia*
	TT5	Działania w złym zamiarze	5.1. *Przechwycenie informacji*
			5.2. *Phishing i spoofing*
			5.3. *Powielanie wiadomości*
			5.4. *Atak siłowy*
			5.5. *Luki w oprogramowaniu*
			5.6. *Ataki na łańcuch dostaw*
			5.7. *Złośliwe oprogramowanie*
			5.8. *Przewidywanie liczb losowych*

Ponadto rejestr zawiera **wykaz bezpośrednich zagrożeń dla portfeli**, z których każde jest powiązane z (niewyczerpującym) wykazem rodzajów ryzyka (sekcja IV).

SEKCJA I

Wysokie ryzyko dla portfeli

R1. Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej

Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej definiuje się jako tworzenie w portfelu tożsamości elektronicznej, która istnieje w świecie rzeczywistym i jest przypisana innemu użytkownikowi. Zasadniczo ryzyko to prowadzi do ryzyka kradzieży tożsamości (R4) i nieupoważnionej transakcji (R9).

R2. Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej

Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej definiuje się jako tworzenie w portfelu tożsamości elektronicznej, która nie istnieje w świecie rzeczywistym.

R3. Tworzenie lub wykorzystywanie fałszywych atrybutów

Tworzenie lub wykorzystywanie fałszywych atrybutów definiuje się jako tworzenie lub wykorzystywanie atrybutów, w przypadku których nie można potwierdzić, że zostały wydane przez wskazanego dostawcę, i którym nie można zaufać.

R4. Kradzież tożsamości

Kradzież tożsamości definiuje się jako nieuprawnione przejęcie jednostki portfela lub utratę czynników uwierzytelniających, co pozwala podszyć się pod daną osobę.

R5. Kradzież danych

Kradzież danych definiuje się jako nieuprawnione pobranie danych. Kradzież danych wiąże się również z zagrożeniami, takimi jak przechwycenie danych (nieupoważnione przechwycenie danych w trakcie przesyłania) i deszyfrowanie danych (nieupoważnione dekodowanie zaszyfrowanych danych), które w niektórych przypadkach mogą prowadzić do ujawnienia danych (R6).

R6. Ujawnienie danych

Ujawnienie danych definiuje się jako nieuprawnione ujawnienie danych osobowych, w tym szczególnych kategorii danych osobowych. Ryzyko naruszenia prywatności jest bardzo podobne, gdy rozważa się je pod kątem prywatności, a nie bezpieczeństwa.

R7. Manipulacja danymi

Manipulację danymi definiuje się jako nieupoważnioną zmianę danych.

R8. Utrata danych

Utratę danych definiuje się jako sytuację, w której dane przechowywane w portfelu zostały utracone w wyniku niewłaściwego użycia lub działania w złej wierze. Ryzyko to jest często ryzykiem wtórnym wobec manipulacji danymi (R7) lub zakłóceń usługi (R13), w przypadku gdy nie można przywrócić całości lub części danych.

R9. Nieupoważniona transakcja

Nieupoważnione transakcje definiuje się jako działania operacyjne prowadzone bez zgody lub wiedzy użytkownika portfela. W wielu przypadkach nieupoważniona transakcja może prowadzić do kradzieży tożsamości (R4) lub ujawnienia danych (R6). Jest to również związane z nieupoważnionymi transakcjami, takimi jak niewłaściwe użycie kluczy kryptograficznych.

R10. Manipulacja transakcją

Manipulację transakcją definiuje się jako nieupoważnioną zmianę operacji w portfelu. Manipulacja transakcją stanowi atak na integralność i wiąże się z naruszeniem integralności danych.

R11. Zaprzeczenie

Zaprzeczenie oznacza sytuację, w której zainteresowana strona zaprzecza wykonaniu określonej czynności lub udziałowi w transakcji, a pozostali interesariusze nie mają dostatecznych dowodów, aby to zakwestionować.

R12. Ujawnienie danych dotyczących transakcji

Ujawnianie danych dotyczących transakcji definiuje się jako ujawnienie informacji na temat transakcji między zainteresowanymi stronami.

R13. Zakłócenie usługi

Zakłócenie usługi definiuje się jako przerwanie lub pogorszenie normalnego działania portfela. Szczególnym rodzajem zakłócenia usługi jest blokada użytkownika, definiowana jako niezdolność użytkownika do dostępu do własnego konta lub portfela.

R14. Inwigilacja

Inwigilację lub monitorowanie definiuje się jako nieupoważnione śledzenie lub obserwowanie działań, komunikacji lub danych użytkownika portfela. Inwigilacja jest często związana z wnioskowaniem, które definiuje się jako dedukcję danych wrażliwych lub osobowych na podstawie pozornie nieszkodliwych informacji.

SEKCJA II

Ryzyko systemowe

Ryzyko systemowe nie jest uwzględniane w wykazie zagrożeń, ponieważ zazwyczaj jest wynikiem wielu zagrożeń, powtarzających się w sposób zagrażający całemu systemowi.

SR1. Inwigilacja hurtowa

Inwigilację hurtową definiuje się jako śledzenie lub obserwowanie działań wielu użytkowników poprzez komunikację lub dane portfela. Inwigilacja hurtowa jest często powiązana z inwigilacją (R14) i wnioskowaniem w skali globalnej, gdy informacje o wielu użytkownikach są łączone, aby wydedukować ich dane wrażliwe lub osobowe bądź zidentyfikować tendencje statystyczne, które można potem wykorzystać do przygotowywania dalszych ataków.

SR2. Nadszarpnięcie reputacji

Nadszarpnięcie reputacji definiuje się jako szkody wizerunkowe organizacji lub organu rządowego. Nadszarpnięcie reputacji powstaje również na skutek innych zagrożeń, gdy naruszenie lub incydent zostanie przedstawiony w mediach, ukazując organizację w niekorzystnym świetle. Nadszarpnięcie reputacji może prowadzić do dalszych zagrożeń, takich jak utrata zaufania wynikająca z uzasadnionych wątpliwości użytkownika oraz utrata ekosystemu, gdy cały ekosystem ulega destabilizacji.

SR3. Niezgodność z przepisami prawa

Niezgodność z przepisami prawa definiuje się jako sytuację, w której nie można przestrzegać odpowiednich przepisów ustawowych, wykonawczych lub norm. W kontekście portfela – zważywszy, że bezpieczeństwo i prywatność rozwiązania są wymaganiami prawnymi – wszystkie zagrożenia mogą prowadzić do pewnego rodzaju niezgodności z przepisami prawa.

SEKCJA III

Zagrożenia techniczne

Zagrożenia techniczne nie zawsze są powiązane z konkretnymi rodzajami ryzyka dla portfeli, ponieważ wiele z nich stanowi środki, które mogą być użyte do przeprowadzenia ataków odpowiadających różnym rodzajom ryzyka.

TT1. Ataki fizyczne

1.1. *Kradzież*

Kradzież definiuje się jako kradzież urządzeń, które mogą wpłynąć na prawidłowe funkcjonowanie portfela (w przypadku gdy urządzenie zostaje skradzione, a jednostka portfela nie jest odpowiednio chroniona). Może się to przyczynić się do powstania wielu rodzajów ryzyka, w tym kradzieży tożsamości (R4), kradzieży danych (R5) i nieupoważnionych transakcji (R9).

1.2. *Wyciek informacji*

Wyciek informacji definiuje się jako nieupoważniony dostęp do informacji, ich ujawnienie lub wymianę po fizycznym dostępie do portfela. Może on w szczególności przyczynić się do ujawnienia danych (R6) i kradzieży danych (R5).

1.3. *Ingerencja*

Ingerencja oznacza naruszenie integralności jednego lub wielu komponentów jednostki portfela lub komponentów, na których dana jednostki portfela polega, np. urządzenia użytkownika lub jego systemu operacyjnego. Może ona w szczególności przyczynić się do manipulacji danymi (R7), utraty danych (R8) i manipulacji transakcją (R10). Ingerencja ukierunkowana na komponenty oprogramowania może przyczynić się do powstania wielu zagrożeń.

TT2. Błędy i błędna konfiguracja

2.1. *Błędy podczas zarządzania systemem informatycznym*

Błędy podczas zarządzania systemem informatycznym oznaczają wyciek informacji, przekazywanie informacji lub szkody spowodowane niewłaściwym wykorzystaniem zasobów informatycznych przez użytkowników (brak wiedzy na temat funkcji aplikacji) lub niewłaściwą konfiguracją bądź błędnym zarządzaniem zasobami informatycznymi.

2.2. *Błędy na poziomie aplikacji lub błędy użytkowania*

Błędy na poziomie aplikacji lub błędy użytkowania definiuje się jako dysfunkcje aplikacji spowodowane błędem w samej aplikacji lub błędem jednego z użytkowników (użytkowników portfela i stron ufających).

2.3. *Błędy na etapie rozwoju i błędne konfiguracje systemu*

Błędy na etapie rozwoju i błędne konfiguracje systemu definiuje się jako dysfunkcje lub słabe punkty spowodowane niewłaściwym opracowaniem lub konfiguracją zasobów informatycznych lub procesów biznesowych (nieodpowiednie specyfikacje produktów informatycznych, nieodpowiednia używalność, niezabezpieczone interfejsy, niewłaściwe działanie polityki i procedur, błędy projektowe).

TT3. Korzystanie z niewiarygodnych zasobów

Korzystanie z niewiarygodnych źródeł definiuje się jako działanie prowadzące do niezamierzonej szkody spowodowanej źle określonymi relacjami zaufania, na przykład zaufania do zewnętrznego dostawcy nieposiadającego odpowiedniego poziomu bezpieczeństwa.

3.1. *Błędne wykorzystanie lub konfiguracja komponentów portfela*

Błędne wykorzystanie lub konfigurację komponentów portfela definiuje się jako niezamierzone uszkodzenie komponentów portfela z powodu błędnego użycia lub niewłaściwej konfiguracji przez użytkowników portfela lub niewystarczająco przeszkolonych deweloperów, lub z powodu braku dostosowania do zmian w krajobrazie zagrożeń, zazwyczaj w związku z używaniem podatnych na zagrożenia komponentów stron trzecich lub platform wykonawczych.

TT4. Awarie i przestoje

4.1. *Awaria lub dysfunkcja sprzętu, urządzeń lub systemów*

Awaria lub dysfunkcja sprzętu oznacza niezamierzone uszkodzenie zasobów informatycznych wynikające z problemów z funkcjonowaniem sprzętu, w tym infrastruktury dostawcy oraz urządzeń użytkowników.

4.2. *Utrata zasobów*

Utratę zasobów definiuje się jako przerwę lub dysfunkcję z powodu niedostępności takich zasobów, np. części do konserwacji.

4.3. *Utrata usług wsparcia*

Utratę usług wsparcia definiuje się jako awarię lub dysfunkcję z powodu niedostępności usług wsparcia wymaganych do właściwego funkcjonowania systemu, z uwzględnieniem łączności sieciowej infrastruktury dostawcy i urządzenia użytkownika.

TT5. Działania w złym zamiarze

5.1. *Przechwycenie informacji*

Przechwycenie informacji oznacza pozyskiwanie niewłaściwie zabezpieczonych informacji podczas transmisji, w tym ataki „człowiek pośrodku".

5.2. *Phishing i spoofing*

Phishing definiuje się jako przechwytywanie informacji, które użytkownik udostępnia w wyniku wprowadzenia w błąd, często powiązanego z fałszowaniem legalnych kanałów komunikacji i stron internetowych. Zagrożenia te są ukierunkowane na użytkownika i zazwyczaj przyczyniają się do kradzieży tożsamości (R4) i nieupoważnionej transakcji (R9), często poprzez kradzież danych (R5) lub ujawnienie danych (R6).

5.3. *Powielanie wiadomości*

Powielanie wiadomości oznacza ponowne wykorzystanie uprzednio przechwyconych komunikatów w celu przeprowadzania nieupoważnionych transakcji, często na poziomie protokołu. To zagrożenie techniczne prowadzi głównie do nieupoważnionych transakcji, które w zależności od transakcji mogą skutkować innymi rodzajami ryzyka.

5.4. *Atak siłowy*

Atak siłowy oznacza naruszenie bezpieczeństwa, najczęściej poufności, poprzez podejmowanie wielu interakcji w celu uzyskania odpowiedzi zawierających przydatne informacje.

5.5. *Luki w oprogramowaniu*

Zagrożenie związane z lukami w oprogramowaniu stanowi naruszenie bezpieczeństwa poprzez wykorzystanie podatności oprogramowania w komponentach portfela lub w komponentach oprogramowania i sprzętu wykorzystywanych do wdrożenia portfela, w tym opublikowanych i niepublikowanych (0-day) podatności na zagrożenia.

5.6. *Ataki na łańcuch dostaw*

Atak na łańcuch dostaw definiuje się jako naruszenie bezpieczeństwa poprzez ataki na podmiot dostarczający dostawcy portfela lub jego użytkowników w celu umożliwienia dalszych ataków na sam portfel.

5.7. *Złośliwe oprogramowanie*

Złośliwe oprogramowanie definiuje się jako naruszenie bezpieczeństwa za pomocą aplikacji wykonujących niepożądane i niezgodne z prawem operacje na portfelu.

5.8. *Przewidywanie liczb losowych*

Przewidywanie liczb losowych definiuje się jako umożliwianie ataków siłowych poprzez częściowe lub całkowite przewidywanie wygenerowanych liczb losowych.

SEKCJA IV

Zagrożenia dla portfeli

Ostatnia sekcja zawiera typowe scenariusze zagrożeń charakterystycznych dla portfeli, które są powiązane z kluczowymi rodzajami wysokiego ryzyka wymienionymi powyżej. Wykaz ten określa zagrożenia, które należy uwzględnić, ale nie stanowi wyczerpującego wykazu zagrożeń, które w dużym stopniu zależą od architektury wybranego rozwiązania w zakresie portfela oraz od ewolucji środowiska zagrożeń. Ponadto w ocenie ryzyka i zaproponowanych środkach dostawca portfela może być odpowiedzialny wyłącznie za komponenty objęte zakresem certyfikacji (*).

ID *Identyfikator*	Opis zagrożenia *Opis zidentyfikowanego zagrożenia* (*)	Nazwa ryzyka *Powiązane ryzyko*
TR1	Atakujący może bez uzasadnionego powodu unieważnić pseudonimy.	Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR2	Atakujący może tworzyć gotowe tożsamości elektroniczne, które nie istnieją.	Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR3	Atakujący może rozpocząć tworzenie nieupoważnionych danych identyfikujących osobę.	Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR4	Atakujący może zwrócić się do administratora o wpis nieprawidłowego dostawcy danych identyfikujących osobę na zaufaną listę dostawcy takich danych.	Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR5	Atakujący może obejść usługę zdalnego potwierdzania tożsamości.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR6	Atakujący może obejść usługę potwierdzającą tożsamość fizyczną.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR7	Atakujący może obejść usługi potwierdzania tożsamości za pomocą (kwalifikowanego) certyfikatu zdalnego.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR8	Atakujący może uzyskać dostęp do portfela, który nie jest związany z daną osobą.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR9	Atakujący może przełamać kontrole techniczne i proceduralne w celu stworzenia niewłaściwych danych identyfikujących osobę.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR10	Atakujący może aktywować nowy portfel na nieprawidłowym bezpiecznym urządzeniu kryptograficznym portfela (WSCD).	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)
TR11	Atakujący może obejść usługę potwierdzania tożsamości związaną z wykorzystaniem istniejących środków eID.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Kradzież tożsamości (R4)/Nieupoważniona transakcja (R9)
TR12	Atakujący może obejść weryfikację przez dostawcę danych identyfikujących osobę potwierdzającą, że portfel jest kontrolowany przez użytkownika, i spowodować wydanie danych identyfikujących osobę do portfela znajdującego się pod kontrolą atakującego.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Kradzież tożsamości (R4)/Nieupoważniona transakcja (R9)

ID *Identyfikator*	Opis zagrożenia *Opis zidentyfikowanego zagrożenia (*)*	Nazwa ryzyka *Powiązane ryzyko*
TR13	Atakujący może otrzymać ważne dane identyfikujące osobę dla nieważnej jednostki portfela.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Kradzież tożsamości (R4)/Nieupoważniona transakcja (R9)
TR14	Dostawca danych identyfikujących osobę może tworzyć sfabrykowane tożsamości, jeśli tożsamość jest związana z istniejącą osobą.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Kradzież tożsamości (R4)/Nieupoważniona transakcja (R9)
TR15	Atakujący może połączyć dane identyfikujące osobę z niewłaściwym portfelem, ponieważ dostawca takich danych nie jest w stanie powiązać ich z prawidłowym portfelem.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Kradzież tożsamości (R4)/Nieupoważniona transakcja (R9)
TR16	Atakujący może upoważnić użytkownika do zatwierdzenia aktywacji nowej jednostki/instancji portfela pod kontrolą atakującego, co pozwala na późniejszą kontrolę poświadczeń.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Tworzenie lub wykorzystywanie fałszywej tożsamości elektronicznej (R2)/Kradzież tożsamości (R4)/Nieupoważniona transakcja (R9)
TR17	Atakujący może utworzyć dane identyfikujące osobę z innego państwa, aby uzyskać dostęp do danych/zasobów cyfrowych obywateli, którzy są celem ataku.	Tworzenie lub wykorzystywanie istniejącej tożsamości elektronicznej (R1)/Kradzież tożsamości (R4)/Nieupoważniona transakcja (R9)
TR18	Atakujący może przełamać kontrole techniczne i proceduralne w celu stworzenia fałszywych (kwalifikowanych) elektronicznych poświadczeń atrybutów ((Q)EAA).	Tworzenie lub wykorzystywanie fałszywych atrybutów (R3)
TR19	Atakujący może przedstawić (Q)EAA, które nie zostały mu wydane zgodnie z prawem.	Tworzenie lub wykorzystywanie fałszywych atrybutów (R3)
TR20	Atakujący może zaatakować kryptograficzny mechanizm portfela ustanawiający połączenie między danymi identyfikującymi osobę a (Q)EAA, które nie powinno być mu wydane.	Tworzenie lub wykorzystywanie fałszywych atrybutów (R3)
TR21	Atakujący może używać (Q)EAA w portfelu, mimo że jego fizyczny odpowiednik wygasł lub jest nieważny.	Tworzenie lub wykorzystywanie fałszywych atrybutów (R3)
TR22	Atakujący może obejść weryfikację przez dostawcę (Q)EAA potwierdzającą, że portfel jest kontrolowany przez użytkownika, i spowodować wydanie takiego poświadczenia dla skompromitowanego portfela znajdującego się pod kontrolą atakującego.	Tworzenie lub wykorzystywanie fałszywych atrybutów (R3)
TR23	Atakujący może fałszować elektroniczne poświadczenia atrybutów.	Tworzenie lub wykorzystywanie fałszywych atrybutów (R3)
TR24	Atakujący może wprowadzić do portfela sfałszowane elektroniczne poświadczenia atrybutów.	Tworzenie lub wykorzystywanie fałszywych atrybutów (R3)
TR25	Portfel może wyświetlać atrybuty stronie ufającej bez zgody użytkownika.	Ujawnienie danych (R6)
TR26	Dane identyfikujące osobę, (Q)EAA lub pseudonimy mogą być przekazane niewłaściwej stronie ufającej.	Ujawnienie danych (R6)
TR27	Atakujący może zainicjować odnowienie elektronicznego poświadczenia atrybutów w złym zamiarze.	Ujawnienie danych (R6)
TR28	Atakujący może skłonić użytkownika do bezprawnego zatwierdzenia wniosku o elektroniczne poświadczenia atrybutów (phishing itp.).	Ujawnienie danych (R6)

ID *Identyfikator*	Opis zagrożenia *Opis zidentyfikowanego zagrożenia (*)*	Nazwa ryzyka *Powiązane ryzyko*
TR29	Atakujący może spowodować wyciek atrybutów z portfela i zidentyfikować użytkownika portfela, jeśli identyfikacja nie jest wymagana/dozwolona.	Ujawnienie danych (R6)
TR30	Atakujący może przełamać kontrole techniczne i proceduralne w celu uzyskania danych.	Ujawnienie danych (R6)
TR31	Atakujący może uzyskać dostęp do żądania.	Ujawnienie danych (R6)
TR32	Atakujący może uzyskać informacje na temat wbudowanych reguł ujawniania atrybutów i przedstawić atrybuty zawarte w aktualnym żądaniu przez jednostki portfela.	Ujawnienie danych (R6)
TR33	Atakujący może uzyskać dostęp do logów lub ich części.	Ujawnienie danych (R6)
TR34	Atakujący może sprawdzić, czy portfel jest zainstalowany na tym samym urządzeniu, którego używa, czy na innym, i zdobyć informacje na jego temat.	Ujawnienie danych (R6)
TR35	Atakujący może zdobyć czynnik wiedzy służący do uwierzytelniania użytkownika w WSCA.	Ujawnienie danych (R6)
TR36	Elektroniczne poświadczenie atrybutów dotyczących osoby, które pojawia się w wielu transakcjach ze stroną ufającą lub między różnymi stronami ufającymi, w sposób niezamierzony umożliwia powiązanie wielu transakcji z właściwą osobą.	Ujawnienie danych (R6)
TR37	Publiczny wykaz unieważnionych poświadczeń/stron ufających może zawierać informacje o wykorzystywaniu poświadczenia przez użytkownika (np. lokalizacja, adres IP itp.).	Ujawnienie danych (R6)
TR38	Nie mogąc udowodnić zgody użytkownika na udostępnienie atrybutów, strony ufające mogą wpłynąć na integralność logów.	Ujawnienie danych (R6)
TR39	Atakujący może niezgodnie z prawem śledzić użytkowników portfela za pomocą niepowtarzalnych/możliwych do śledzenia identyfikatorów.	Ujawnienie danych (R6)/Inwigilacja (R14)
TR40	Strona ufająca składająca się z wielu jednostek/podmiotów, z których każdy ma inny zakres dozwolonych żądań/procesów, może żądać danych i przetwarzać dane, do których nie ma prawnych podstaw.	Ujawnienie danych (R6)/Nieupoważniona transakcja (R9)
TR41	Atakujący może zakłócić kontrole integralności i autentyczności w portfelu danych identyfikujących osobę, tak aby zawsze kończyły się powodzeniem.	Manipulacja danymi (R7)
TR42	Atakujący może obejść lub zakłócić przeprowadzane przez portfel kontrole weryfikujące integralność i autentyczność żądanych atrybutów, tak aby zawsze kończyły się powodzeniem.	Manipulacja danymi (R7)
TR43	Atakujący może obejść lub zakłócić przeprowadzane przez portfel kontrole weryfikujące wszystkie żądane atrybuty należące do tego samego użytkownika, tak aby zawsze kończyły się powodzeniem.	Manipulacja danymi (R7)
TR44	Atakujący może obejść lub zakłócić przeprowadzane przez portfel kontrole weryfikujące ważność danych identyfikujących osobę oraz to, czy zostały wydane przez zaufanego dostawcę, tak by zawsze kończyły się powodzeniem.	Manipulacja danymi (R7)

ID *Identyfikator*	Opis zagrożenia *Opis zidentyfikowanego zagrożenia* (*)	Nazwa ryzyka *Powiązane ryzyko*
TR45	Atakujący może obejść lub zakłócić przeprowadzane przez portfel kontrole weryfikujące ważność (Q)EAA oraz to, czy poświadczenie zostało wydane przez kwalifikowanego dostawcę usług zaufania, tak aby zawsze kończyły się powodzeniem.	Manipulacja danymi (R7)
TR46	Atakujący może obejść lub zakłócić przeprowadzane przez portfel kontrole weryfikujące, czy dane identyfikujące osobę zostały unieważnione przez dostawcę, tak aby zawsze kończyły się powodzeniem.	Manipulacja danymi (R7)
TR47	Atakujący może obejść lub zakłócić przeprowadzane przez portfel kontrole weryfikujące, czy (Q)EAA zostało unieważnione przez dostawcę tego (Q)EAA, tak aby zawsze kończyły się powodzeniem.	Manipulacja danymi (R7)
TR48	Atakujący może modyfikować treść kopii zapasowych i odzyskanych danych, które powinny znajdować się wyłącznie pod kontrolą użytkownika.	Manipulacja danymi (R7)/Utrata danych (R8)
TR49	Atakujący może zmienić historię transakcji danej instancji portfela na poziomie rejestru aktywności.	Manipulacja danymi (R7)/Utrata danych (R8)
TR50	Atakujący może podsłuchiwać połączenie między portfelem a stroną ufającą.	Kradzież danych (R5)/Ujawnianie danych (R6)
TR51	Atakujący może nakłonić użytkownika do przekazania danych osobowych (tj. dane identyfikujące osobę, elektroniczne poświadczenia atrybutów, pseudonimy, podpisy elektroniczne, logi i inne dane) atakującemu lub osobie trzeciej, której nie zamierzał ich ujawniać.	Kradzież danych (R5)/Ujawnianie danych (R6)
TR52	Atakujący może odczytać historię transakcji dla danej instancji portfela z rejestrów aktywności.	Kradzież danych (R5)/Ujawnianie danych (R6)
TR53	Atakujący może eksportować lub wydobywać kryptograficzną zawartość klucza poza WSCD.	Kradzież danych (R5)/Ujawnianie danych (R6)/Nieupoważniona transakcja (R9)
TR54	Atakujący może odczytać treść kopii zapasowych i odzyskanych danych, które powinny znajdować się wyłącznie pod kontrolą użytkownika.	Kradzież danych (R5)/Ujawnianie danych (R6)
TR55	Atakujący może obejść metodę uwierzytelniania użytkownika, aby użyć pseudonimu wygenerowanego przez jednostkę portfela.	Kradzież tożsamości (R4)
TR56	Atakujący może zaoferować użytkownikom aplikację, która imituje ważny portfel.	Kradzież tożsamości (R4)
TR57	Atakujący może eksportować dane dotyczące portfela, w tym dane identyfikujące osobę, (Q)EAA lub logi.	Kradzież tożsamości (R4)
TR58	Atakujący może eksportować materiał powiązania kryptograficznego.	Kradzież tożsamości (R4)
TR59	Atakujący może przejąć tożsamość za pomocą kluczy kryptograficznych portfela.	Kradzież tożsamości (R4)
TR60	Atakujący może skopiować jednostkę osobistego portfela innego użytkownika na swoje urządzenie i ją wykorzystać.	Kradzież tożsamości (R4)/Tworzenie lub wykorzystanie istniejącej tożsamości elektronicznej (R1)

ID *Identyfikator*	Opis zagrożenia *Opis zidentyfikowanego zagrożenia* (*)	Nazwa ryzyka *Powiązane ryzyko*
TR61	Organy innego państwa mogą zażądać od użytkownika pokazania lub udostępnienia wszystkich danych portfela w sytuacji zbliżeniowej, takiej jak przekraczanie granicy tego państwa.	Kradzież tożsamości (R4)/Inwigilacja (R14)
TR62	Po awarii urządzenia użytkownika, użytkownicy nie mogą przenieść swoich rejestrów transakcji, co skutkuje brakiem możliwości identyfikacji poprzednich transakcji w nowym portfelu.	Zaprzeczenie (R11)
TR63	Użytkownicy nie mogą odzyskać swoich rejestrów transakcji po awarii urządzenia użytkownika, co skutkuje brakiem możliwości śledzenia danych w nowym portfelu.	Zaprzeczenie (R11)
TR64	Strony ufające mogą mieć trudności z udowodnieniem zgody na zdalne podpisy elektroniczne.	Zaprzeczenie (R11)
TR65	Atakujący może przeciążyć sieć dużą liczbą żądań podczas połączenia ze stronami ufającymi.	Zakłócenie usługi (R13)
TR66	Atakujący może przeciążyć usługę udostępniania statusu połączeniami ze stronami ufającymi.	Zakłócenie usługi (R13)
TR67	Atakujący może sprawić, że atrybut pojawi się jako kwestionowany/odrzucony, mimo że został przedstawiony jako ważny.	Zakłócenie usługi (R13)
TR68	Atakujący może unieważnić dane identyfikujące osobę bez uzasadnionego powodu.	Zakłócenie usługi (R13)
TR69	Atakujący może unieważnić dane identyfikujące osobę bez zgody użytkownika.	Zakłócenie usługi (R13)
TR70	Atakujący może unieważnić (Q)EAA bez uzasadnionego powodu.	Zakłócenie usługi (R13)
TR71	Atakujący może unieważnić (Q)EAA bez zgody użytkownika.	Zakłócenie usługi (R13)
TR72	Atakujący może wywołać wiele żądań identyfikacji, które nie będą rozpoznawane jako celowe żądania osierocone.	Zakłócenie usługi (R13)
TR73	Atakujący może uruchomić wiele żądań bez dalszych transakcji.	Zakłócenie usługi (R13)
TR74	Atakujący może pozwolić stronie ufającej na żądanie identyfikacji bez pasującej odpowiedzi identyfikacyjnej oraz bez pełnej kontroli.	Zakłócenie usługi (R13)
TR75	Atakujący może wysłać odpowiedź na żądanie po upływie czasu oczekiwania lub w podobnych sytuacjach prowadzących do zakłócenia usługi.	Zakłócenie usługi (R13)
TR76	Strona ufająca może wysłać wiele nieważnych żądań.	Zakłócenie usługi (R13)
TR77	Atakujący może wysłać wiele nieważnych żądań do dostawcy portfela.	Zakłócenie usługi (R13)
TR78	Atakujący może uniemożliwić państwu członkowskiemu usunięcie niewiarygodnego dostawcy danych identyfikujących osobę z zaufanej listy zaufanych dostawców danych identyfikujących osobę.	Zakłócenie usługi (R13)
TR79	Atakujący może uniemożliwić zawieszenie lub unieważnienie portfela.	Zakłócenie usługi (R13)

ID *Identyfikator*	Opis zagrożenia *Opis zidentyfikowanego zagrożenia* (*)	Nazwa ryzyka *Powiązane ryzyko*
TR80	Atakujący może zablokować transakcje realizowane przez strony ufające, użytkowników lub dostawcę danych identyfikujących osobę.	Zakłócenie usługi (R13)
TR81	Atakujący może zablokować lub uniemożliwić dostęp do WSCD.	Zakłócenie usługi (R13)
TR82	Atakujący może uniemożliwić dostawcy danych identyfikujących osobę unieważnienie lub zawieszenie danych identyfikujących osobę.	Zakłócenie usługi (R13)/Nieupoważniona transakcja (R9)
TR83	Strona ufająca może wywnioskować dane tożsamości użytkownika bez informacji, które zostały jej przekazane.	Inwigilacja (R14)
TR84	Grupa stron ufających lub dostawców danych identyfikujących osobę może wywnioskować dane tożsamości użytkownika bez informacji, które zostały jej przekazane.	Inwigilacja (R14)
TR85	Atakujący może wyśledzić i namierzyć użytkownika, wykorzystując jego dane identyfikujące osobę, w przypadku gdy identyfikacja użytkownika nie jest wymagana.	Inwigilacja (R14)
TR86	Atakujący może utworzyć „fałszywą” prezentację kombinacji (Q)EAA	Manipulacja transakcją (R10)
TR87	Atakujący może aktywować/przejąć portfel zdalnie (np. aplikacja bankowa zawierająca żądanie uwierzytelnienia lub atestacji), bez wyraźnej zgody lub wyłącznej kontroli użytkownika, w sytuacji, gdy użytkownik nie jest świadomy (np. podczas snu) lub nie może zobaczyć strony ufającej.	Manipulacja transakcją (R10)
TR88	Atakujący mogą wprowadzać zmiany w metadanych żądania (nazwa usługi, zastosowania itp.).	Manipulacja transakcją (R10)
TR89	Atakujący mogą wprowadzać zmiany w informacjach zwrotnych (stan usługi, wartość jednorazowa itp.).	Manipulacja transakcją (R10)
TR90	Atakujący mogą wprowadzać zmiany w informacjach o atrybutach żądania (np. nadmierne zadawanie pytań itp.).	Manipulacja transakcją (R10)
TR91	Strona ufająca może odtworzyć elementy z poprzedniej sesji podczas innej sesji.	Manipulacja transakcją (R10)
TR92	Atakujący może zastąpić lub zmodyfikować dane identyfikujące osobę podczas ich przesyłania przez dostawcę danych identyfikujących osobę do jednostki portfela.	Manipulacja transakcją (R10)
TR93	Atakujący może zastąpić lub zmodyfikować dane identyfikujące osobę podczas ich przesyłania z jednostki portfela do strony ufającej online.	Manipulacja transakcją (R10)
TR94	Atakujący może zastąpić lub zmodyfikować dane identyfikujące osobę podczas ich przesyłania z jednostki portfela do strony ufającej offline.	Manipulacja transakcją (R10)
TR95	Atakujący może wydać dane identyfikujące osobę bez zgody użytkownika.	Nieupoważniona transakcja (R9)
TR96	Atakujący może użyć unieważnionych lub nieważnych wbudowanych reguł ujawniania, potencjalnie bez wiedzy stron ufających.	Nieupoważniona transakcja (R9)
TR97	Atakujący może „przekonać” portfel do weryfikacji błędnych podpisów elektronicznych.	Nieupoważniona transakcja (R9)
TR98	Atakujący może korzystać z portfela poza kontrolą użytkownika.	Nieupoważniona transakcja (R9)

ID *Identyfikator*	Opis zagrożenia *Opis zidentyfikowanego zagrożenia* (*)	Nazwa ryzyka *Powiązane ryzyko*
TR99	Atakujący może przekonać użytkownika do uwierzytelnienia i zatwierdzenia transakcji z atakującym lub nieupoważnioną osobą trzecią.	Nieupoważniona transakcja (R9)
TR100	Atakujący może nakłonić użytkownika do złożenia podpisu elektronicznego bez przedstawienia mu treści lub po przedstawieniu mu błędnych treści.	Nieupoważniona transakcja (R9)
TR101	Atakujący może ominąć kontrolę dostępu do konta użytkownika za pomocą dostawcy portfela.	Nieupoważniona transakcja (R9)
TR102	Atakujący może udawać strony ufające podczas połączeń ze stronami ufającymi.	Nieupoważniona transakcja (R9)/Ujawnianie danych (R6)
TR103	Użytkownik korzystający z przeglądarki do połączenia się ze stroną ufającą może się różnić od użytkownika korzystającego w tym celu z portfela.	Nieupoważniona transakcja (R9)/Ujawnianie danych (R6)/Kradzież tożsamości (R4)
TR104	Atakujący może przekonać użytkownika do unieważnienia portfela bez powodu.	Nieupoważniona transakcja (R9)/Zakłócenie usługi (R13)
TR105	Atakujący może dokonywać ataków „człowiek pośrodku”.	Nieupoważniona transakcja (R9)/Ujawnianie danych (R6)/Inwigilacja (R14)
TR106	Atakujący może przedstawić nieważne lub unieważnione atrybuty z portfela, który nie łączy się regularnie z siecią.	Wpływ na różne rodzaje ryzyka
TR107	Atakujący może dokonać kradzieży danych użytkownika przez spoofing portfela.	Wpływ na różne rodzaje ryzyka
TR108	Atakujący może podszyć się pod użytkownika, powtarzając/imitując żądanie danych (np. uwierzytelnienie), aby sprawić wrażenie, że jest ono poprawne.	Wpływ na różne rodzaje ryzyka
TR109	Atakujący może odtworzyć wbudowane reguły ujawniania informacji wobec użytkownika, imitując zatwierdzone żądanie.	Wpływ na różne rodzaje ryzyka
TR110	Atakujący może wykorzystać brak informacji użytkowników portfela lub nieuzasadnione opóźnienia po naruszeniu bezpieczeństwa lub złamaniu zabezpieczeń.	Wpływ na różne rodzaje ryzyka
TR111	Atakujący może zmodyfikować wcześniej zainstalowaną, oryginalną instancję portfela, aby dodać złośliwe funkcje.	Wpływ na różne rodzaje ryzyka
TR112	Atakujący może zmodyfikować oryginalną instancję portfela i przedstawić ją użytkownikom jako zgodną z prawidłową.	Wpływ na różne rodzaje ryzyka
TR113	Atakujący może złamać mechanizm uwierzytelniania tożsamości użytkownika, aby obejść proces uwierzytelniania użytkownika portfela.	Wpływ na różne rodzaje ryzyka
TR114	Atakujący może podczas wdrażania portfela na urządzeniu użytkownika wprowadzić złośliwy kod lub backdoor.	Wpływ na różne rodzaje ryzyka
TR115	Atakujący może podczas opracowywania portfela wprowadzić złośliwy kod lub backdoor.	Wpływ na różne rodzaje ryzyka
TR116	Atakujący może manipulować generowaniem liczb losowych, aby wystarczająco obniżyć ich entropię, co umożliwia przeprowadzenie ataków.	Wpływ na różne rodzaje ryzyka

ID *Identyfikator*	Opis zagrożenia *Opis zidentyfikowanego zagrożenia* (*)	Nazwa ryzyka *Powiązane ryzyko*
TR117	Atakujący może ingerować w urządzenia użytkownika w łańcuchu dostaw, aby uwzględnić kod lub konfiguracje, które nie spełniają warunków użytkowania portfela.	Wpływ na różne rodzaje ryzyka
TR118	Atakujący może aktywować jednostkę portfela, korzystając ze sfałszowanego WSCD kontrolowanego przez atakujących.	Wpływ na różne rodzaje ryzyka
TR119	Atakujący może czytać informacje przesyłane do WSCA lub WSCD.	Wpływ na różne rodzaje ryzyka
TR120	Atakujący może wysyłać dowolne informacje do WSCA.	Wpływ na różne rodzaje ryzyka
TR121	Atakujący może dokonać kradzieży danych, przechwytując informacje wymieniane między WSCA a WSCD.	Wpływ na różne rodzaje ryzyka
TR122	Atakujący może wysyłać dowolne informacje do WSCD.	Wpływ na różne rodzaje ryzyka
TR123	Atakujący może wysłać informacje do WSCD, omijając WSCA.	Wpływ na różne rodzaje ryzyka
TR124	Atakujący może wykorzystać technikę phishingu, aby skierować użytkowników do fałszywego portfela i aplikacji odpowiedzialnych za zarządzanie danymi identyfikującymi osobę.	Wpływ na różne rodzaje ryzyka
TR125	Atakujący może zastąpić klucze portfela innymi kluczami, aby stworzyć wiadomości do wykorzystania w innym ataku.	Wpływ na różne rodzaje ryzyka
TR126	Atakujący może modyfikować lub niszczyć klucze portfela, co sprawia, że niektóre funkcje portfela stają się bezużyteczne.	Wpływ na różne rodzaje ryzyka
TR127	Atakujący może kontrolować złośliwe oprogramowanie, aby uzyskać dostęp do danych przechowywanych w portfelu.	Wpływ na różne rodzaje ryzyka
TR128	Atakujący może uzyskać dostęp do dowodów wygenerowanych w portfelu.	Wpływ na różne rodzaje ryzyka
TR129	Dostawcy portfela mają dostęp do obiektów znajdujących się w portfelu.	Wpływ na różne rodzaje ryzyka
TR130	Dostawcy portfela mogą uzyskać dostęp do dowodów wygenerowanych w portfelu.	Wpływ na różne rodzaje ryzyka
TR131	Atakujący może dokonać kradzieży odblokowanego urządzenia portfela.	Wpływ na różne rodzaje ryzyka
TR132	Atakujący może manipulować systemem, aby zapobiec rejestrowaniu określonych zdarzeń.	Wpływ na różne rodzaje ryzyka
TR133	Atakujący może przechwytywać komunikację między instancją portfela a WSCA lub odtwarzać/imitować użytkownika (np. za pomocą mechanizmu uwierzytelniania).	Wpływ na różne rodzaje ryzyka

ZAŁĄCZNIK II

KRYTERIA OCENY DOPUSZCZALNOŚCI INFORMACJI NA TEMAT BEZPIECZEŃSTWA

Nazwa	Cel	Kwestie, na które warto zwrócić uwagę
EUCC	Produkty ICT	Informacje na temat wydawcy: brak (akredytowane jednostki certyfikujące) Zakres stosowania: — sprawdzenie profilu ochrony i celu zabezpieczeń; — sprawdzenie poziomu bezpieczeństwa oceny i rozszerzeń. Kwestie bezpieczeństwa: — sprawdzenie ograniczeń w dokumentacji użytkownika; — w przypadku kompozycji może być wymagany dostęp do raportu technicznego z oceny.
Europejski program certyfikacji cyberbezpieczeństwa dla usług w chmurze (EUCS) (jeśli dostępny)	Usługi w chmurze	Informacje na temat wydawcy: brak (akredytowane jednostki certyfikujące) Zakres stosowania: — sprawdzenie opisu usługi w chmurze; — sprawdzenie poziomu oceny i profili rozszerzenia. Kwestie bezpieczeństwa: — sprawdzenie informacji dotyczących przejrzystości oraz – w razie potrzeby – informacji dotyczących kompozycji.
Programy certyfikacji cyberbezpieczeństwa funkcjonujące w UE, w tym programy SOG-IS	Produkty ICT	Informacje na temat wydawcy: brak (państwa członkowskie) Zakres stosowania: — sprawdzenie profilu ochrony i celu zabezpieczeń; — sprawdzenie poziomu bezpieczeństwa oceny i rozszerzeń. Kwestie bezpieczeństwa: — sprawdzenie ograniczeń w dokumentacji użytkownika; — w przypadku kompozycji może być wymagany dostęp do raportu technicznego z oceny.
EN 17640:2018 (FITCEM, w tym CSPN, BSZ, LINCE, BSZA)	Produkty ICT	Informacje na temat wydawcy: — sprawdzenie programu i wymogów dotyczących jednostek certyfikujących. Zakres stosowania: — sprawdzenie opisu produktu; — sprawdzenie wniosków o zabezpieczenie; — sprawdzenie poziomu bezpieczeństwa. Kwestie bezpieczeństwa: — sprawdzenie wykonanych czynności i ustaleń zawartych w raporcie;
programy certyfikacji kwalifikowanych urządzeń do składania podpisu zgodnie z art. 30 rozporządzenia (UE) nr 910/2014.	Kwalifikowane urządzenie do składania podpisu (QSCD)	Informacje na temat wydawcy: — sprawdzenie programu i wymogów dotyczących jednostek certyfikujących. Zakres stosowania: — sprawdzenie opisu produktu; — sprawdzenie wniosków o zabezpieczenie; — sprawdzenie poziomu bezpieczeństwa. Kwestie bezpieczeństwa: — sprawdzenie wykonanych czynności.

Nazwa	Cel	Kwestie, na które warto zwrócić uwagę
EN ISO/IEC 27001:2022	SZBI	Informacje na temat wydawcy: brak (akredytowane jednostki certyfikujące) Zakres stosowania: — sprawdzenie opisu systemu zarządzania; — sprawdzenie deklaracji stosowania. Kwestie bezpieczeństwa: — sprawdzenie wykonanych czynności.
SOC2	Organizacje	Informacje na temat wydawcy: — sprawdzenie statusu księgowego. Zakres stosowania: — sprawdzenie oświadczenia kierownictwa i opisu kontroli; — sprawdzenie deklaracji stosowania. Kwestie bezpieczeństwa: — sprawdzenie ustaleń zawartych w sprawozdaniu; — w razie potrzeby sprawdzenie pism pomostowych.
MDSCert (GSMA) (jeżeli jest dostępny)	Urządzenia mobilne	Informacje na temat wydawcy: — sprawdzenie wymogów dotyczących jednostek certyfikujących. Zakres stosowania: — sprawdzenie poziomu bezpieczeństwa zabezpieczenia. — sprawdzenie wymogów programu. Kwestie bezpieczeństwa: — sprawdzenie czynności i ustaleń zawartych w raporcie.
Inne programy	Dowolny komponent	Informacje o programie: — sprawdzenie adekwatności i przepisów programu. Informacje na temat wydawcy: — sprawdzenie wymogów dotyczących jednostek certyfikujących. Zakres stosowania: — sprawdzenie wymogów programu; — sprawdzenie celu zabezpieczeń lub podobnego dokumentu opisującego wymogi w zakresie funkcjonalności i zapewnienia bezpieczeństwa; — sprawdzenie opisu produktu i wybranych wymogów funkcjonalnych w zakresie bezpieczeństwa. Kwestie bezpieczeństwa: — sprawdzenie czynności i ustaleń zawartych w raporcie.

ZAŁĄCZNIK III

WYMAGANIA FUNKCJONALNE DOTYCZĄCE ROZWIĄZAŃ W ZAKRESIE PORTFELA

Zgodnie z art. 5a ust. 4, 5, 8 i 14 rozporządzenia (UE) nr 910/2014 kryteria funkcjonalne, jakie musi spełniać certyfikowane rozwiązanie w zakresie portfela oraz system identyfikacji elektronicznej, w ramach którego jest ono zapewniane, obejmują wymogi funkcjonalne dotyczące operacji wymienionych w poniższych punktach:

1) Rozporządzenie wykonawcze Komisji (UE) 2024/2979 ([1]) ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji;

2) Rozporządzenie wykonawcze Komisji (UE) 2024/2982 ([2]) ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do protokołów i interfejsów, które mają być obsługiwane przez europejskie ramy tożsamości cyfrowej;

3) Rozporządzenie wykonawcze Komisji (UE) 2024/2977 ([3]) ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej.

([1]) Rozporządzenie wykonawcze Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji (Dz.U. L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Rozporządzenie wykonawcze Komisji (UE) 2024/2982 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do protokołów i interfejsów, które mają być obsługiwane przez europejskie ramy tożsamości cyfrowej (Dz.U. L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Rozporządzenie wykonawcze Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz.U. L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

ZAŁĄCZNIK IV

METODY I PROCEDURY DOTYCZĄCE DZIAŁAŃ W ZAKRESIE OCENY

1. **Kontrola wdrożenia rozwiązania w zakresie portfela**

Ocena zgodności polega na wyborze konkretnych działań w zakresie oceny.

Krajowe programy certyfikacji określają działania w zakresie oceny w celu zbadania dostarczonych informacji, uwzględniając co najmniej następujące elementy:

a) analizę dostarczonych informacji w celu potwierdzenia, że są one odpowiednie dla jednej z architektur określonych w krajowych programach certyfikacji;

b) analizę zakresu ryzyka w cyberprzestrzeni i zagrożeń cyberbezpieczeństwa zidentyfikowanych w rejestrze ryzyka w załączniku I za pomocą opisanych środków kontroli bezpieczeństwa.

Analiza, o której mowa w lit. a)–b), opiera się na podstawach i uzasadnieniu dostarczonych przez dostawcę portfela.

2. **Działania w zakresie oceny związane z bezpiecznym urządzeniem kryptograficznym portfela**

1) Operacje krytyczne, w tym obliczenia kryptograficzne, nie muszą być w pełni wdrożone w WSCD. Jednak część wdrożona w WSCD, funkcjonująca w ramach rozwiązania w zakresie portfela, powinna gwarantować ochronę kluczowych operacji przed atakami ze strony atakujących dysponujących wysokim potencjałem ataku, zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2015/1502 ([1]).

2) WSCD lub jego część może być przedmiotem certyfikacji, jeśli dostarczona przez posiadacza certyfikatu lub wnioskodawcę, lub wyłączona z zakresu certyfikacji, gdy znajduje się w urządzeniu dostarczonym przez użytkownika końcowego. Ponadto krajowe programy certyfikacji określają działania w zakresie oceny w celu weryfikacji odpowiedniości WSCD w dwóch następujących przypadkach:

   a) jeżeli WSCA zależy od konkretnego WSCD (tj. jeśli należy go ocenić jako produkt złożony na podstawie WSCD), ocena WSCA wymaga dostępu do dodatkowych informacji związanych z certyfikacją WSCD, w tym w szczególności do raportu technicznego z oceny;

   b) jeżeli architektura rozważana w programie wykorzystuje kilka WSCD lub jeżeli niektóre operacje na aktywach krytycznych są wykonywane poza WSCD, krajowe programy certyfikacji powinny obejmować działania w zakresie oceny w celu zapewnienia, aby rozwiązanie w ujęciu ogólnym oferowało oczekiwany poziom bezpieczeństwa.

3) Warunkiem wstępnym certyfikacji w ramach krajowych programów certyfikacji jest ocena WSCD pod kątem wymogów dotyczących wysokiego poziomu bezpieczeństwa określonych w rozporządzeniu wykonawczym (UE) 2015/1502.

   a) Jeżeli spełniono warunki określone w art. 3 ust. 3 lit. b), ocena WSCD lub jego części obejmuje ocenę podatności na zagrożenia określoną w normie EN ISO/IEC 15408-3:2022 na poziomie AVA_VAN.5, zgodnie z załącznikiem I do rozporządzenia wykonawczego Komisji (UE) 2024/482 ([2]), chyba że dostatecznie uzasadniono jednostce certyfikującej, że charakterystyka bezpieczeństwa WSCA umożliwia zastosowanie niższego poziomu oceny przy jednoczesnym utrzymaniu tego samego ogólnego wysokiego poziomu bezpieczeństwa, jak określono w rozporządzeniu wykonawczym (UE) 2015/1502.

([1]) Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 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 235 z 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/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).

4) Ponadto w dokumentacji dotyczącej każdej konkretnej architektury krajowe programy certyfikacji określają założenia dotyczące tej oceny WSCD, na podstawie których można zapewnić odporność na atakujących dysponujących wysokim potencjałem ataku, zgodnie z rozporządzeniem wykonawczym (UE) 2015/1502, oraz wskazywać działania w zakresie oceny w celu potwierdzenia tych założeń i weryfikacji po wydaniu zaświadczenia, że założenia nadal są spełniane. Systemy krajowe powinny także wymagać, aby kandydaci do certyfikacji doprecyzowali te założenia dla konkretnej implementacji oraz opisali wprowadzone środki w celu zagwarantowania, że założenia będą weryfikowane przez cały okres trwania certyfikacji.

5) Wszystkie krajowe programy certyfikacji muszą obejmować działania w zakresie oceny ukierunkowane na zweryfikowanie, że informacje na temat bezpieczeństwa, do których ma dostęp WSCD, są odpowiednie dla celów rozwiązania w zakresie portfela, poprzez analizę tych informacji, w tym danych na temat celu zabezpieczeń dla certyfikatów EUCC, z uwzględnieniem następujących działań:

   a) sprawdzenie, czy zakres oceny jest odpowiedni, co w przypadku certyfikatów EUCC oznacza na przykład zweryfikowanie, czy cel w zakresie bezpieczeństwa jest zgodny z jednym z profili zabezpieczeń zalecanych w EUCC;

   b) sprawdzenie, czy założenia dotyczące środowiska operacyjnego są zgodne z rozwiązaniem w zakresie portfela, co na przykład w przypadku certyfikatów EUCC oznacza, że założenia te można znaleźć w celu zabezpieczeń;

   c) sprawdzenie, czy zalecenia zawarte w wytycznych dla użytkownika lub w dokumentacji są zgodne z warunkami, na jakich WSCD ma być stosowane w rozwiązaniu w zakresie portfela;

   d) sprawdzenie, czy założenia przyjęte w krajowym programie certyfikacji w odniesieniu do WSCD zostały zweryfikowane i uwzględnione w informacjach na temat bezpieczeństwa.

6) W przypadkach, gdy niektóre weryfikacje nie są wystarczająco rozstrzygające, krajowe programy certyfikacji wymagają od jednostek certyfikujących określenia wymogów kompensacyjnych na potrzeby bezpiecznej aplikacji kryptograficznej portfela (WSCA), bazujących na WSCD, które będą uwzględnione w ocenie WSCA. Jeżeli nie jest to możliwe, krajowe programy certyfikacji uznają WSCD za nieodpowiednie, co oznacza, że certyfikat zgodności rozwiązania w zakresie portfela nie zostanie wydany.

3. **Działania w zakresie oceny dotyczące bezpiecznej aplikacji kryptograficznej portfela (WSCA)**

1) Krajowe programy certyfikacji wymagają, aby WSCA, jako część rozwiązania w zakresie portfela, była oceniana pod kątem wymogów co najmniej wysokiego poziomu bezpieczeństwa określonych w rozporządzeniu wykonawczym (UE) 2015/1502.

2) Ocena ta obejmuje ocenę podatności na zagrożenia, jak określono w normie EN ISO/IEC 15408-3:2022 na poziomie AVA_VAN.5, zgodnie z załącznikiem I do rozporządzenia wykonawczego (UE) 2024/482, chyba że dostatecznie uzasadniono jednostce certyfikującej, że charakterystyka bezpieczeństwa WSCA umożliwia zastosowanie niższego poziomu oceny przy jednoczesnym utrzymaniu takiego samego ogólnego wysokiego poziomu bezpieczeństwa, jak wskazano w rozporządzeniu wykonawczym (UE) 2015/1502.

3) Gdy WSCA nie jest zapewniana przez dostawcę portfela, krajowe programy certyfikacji określają założenia dotyczące tej oceny WSCA, na podstawie których można zapewnić odporność na atakujących dysponujących wysokim potencjałem ataku, zgodnie z rozporządzeniem wykonawczym (UE) 2015/1502, oraz wskazywać działania w zakresie oceny w celu potwierdzenia tych założeń i weryfikacji po wydaniu zaświadczenia, że założenia nadal są spełniane. Systemy krajowe powinny także wymagać, aby kandydaci do certyfikacji doprecyzowali te założenia dla konkretnej implementacji oraz opisali wprowadzone środki w celu zagwarantowania, że założenia będą weryfikowane przez cały okres trwania certyfikacji.

4) Wszystkie krajowe programy certyfikacji muszą obejmować działania w zakresie oceny ukierunkowane na zweryfikowanie, że informacje na temat bezpieczeństwa, do których ma dostęp WSCA, są odpowiednie dla celów rozwiązania w zakresie portfela, poprzez analizę tych informacji, w tym danych na temat celu zabezpieczeń dla certyfikatów EUCC, z uwzględnieniem następujących działań:

   a) sprawdzenie, czy zakres oceny jest odpowiedni, co w przypadku certyfikatów EUCC oznacza na przykład zweryfikowanie, czy cel w zakresie bezpieczeństwa jest zgodny z jednym z profili zabezpieczeń zalecanych w EUCC;

   b) sprawdzenie, czy założenia dotyczące środowiska operacyjnego są zgodne z rozwiązaniem w zakresie portfela, co na przykład w przypadku certyfikatów EUCC oznacza, że założenia te można znaleźć w celu zabezpieczeń;

c) sprawdzenie, czy zalecenia zawarte w wytycznych dla użytkownika lub w dokumentacji są zgodne z warunkami, na jakich WSCA ma być stosowane w rozwiązaniu w zakresie portfela;

d) sprawdzenie, czy założenia przyjęte w krajowym programie certyfikacji w odniesieniu do WSCA zostały zweryfikowane i uwzględnione w informacjach na temat bezpieczeństwa.

5) Krajowe programy certyfikacji wymagają, aby ocena WSCA obejmowała wszystkie środki kontroli w zakresie ochrony wdrożone przez WSCA.

4. **Działania w zakresie oceny dotyczące urządzenia użytkownika końcowego**

Ze względu na fakt, że rejestr ryzyka, określony w załączniku I do niniejszego rozporządzenia, identyfikuje ryzyko, które jest bezpośrednio związane z bezpieczeństwem urządzenia użytkownika końcowego, krajowe programy certyfikacji określają wymogi bezpieczeństwa dla urządzeń użytkownika końcowego. Z uwagi na fakt, że urządzenia te są dostarczane przez użytkownika końcowego, a nie przez dostawcę portfela, powyższe wymogi powinny jednak być objęte założeniami.

W odniesieniu do każdego założenia rozwiązanie w zakresie portfela powinno zawierać mechanizm umożliwiający weryfikację w odniesieniu do każdej jednostki portfela, że urządzenie użytkownika końcowego spełnia to założenie. Mechanizmy te powinny być traktowane jako środki zabezpieczające i uwzględnione w działaniach w zakresie oceny w celu wykazania ich odpowiedniości i skuteczności na właściwym poziomie bezpieczeństwa.

Poniżej przedstawiono dwa przykłady:

a) urządzenie użytkownika końcowego może zawierać certyfikowane WSCD, co należy wykazać. Zazwyczaj odbywa się to za pomocą mechanizmu kryptograficznego w celu weryfikacji obecności w certyfikowanym WSCD hasła kryptograficznego, które jest dostępne wyłącznie w certyfikowanym WSCD. W takim przypadku hasło kryptograficzne należy uznać za składnik aktywów krytycznych i objąć certyfikacją WSCD lub WSCA;

b) typowym wymogiem dla urządzeń użytkownika końcowego jest wymóg, aby urządzenia te otrzymywały aktualizacje zabezpieczeń. Z uwagi na fakt, że wymóg ten dotyczy instancji portfela, mechanizm weryfikacji dostępności aktualizacji zabezpieczeń musi być objęty działaniami w zakresie oceny na poziomie bezpieczeństwa odpowiednim dla instancji portfela, zwłaszcza że prawdopodobnie będzie zintegrowany z tą instancją portfela.

5. **Działania w zakresie oceny dotyczące instancji portfela**

1) W ocenie instancji portfela uwzględnia się następujące dwa najważniejsze wyzwania:

a) instancja portfela prawdopodobnie występuje w zbiorze wariantów tej samej aplikacji bazowej, przy czym każdy wariant jest dostosowywany do konkretnej kategorii urządzeń użytkownika końcowego;

b) poszczególne warianty instancji portfela będą prawdopodobnie potrzebowały częstych aktualizacji, aby śledzić rozwój podstawowej platformy zabezpieczeń, na przykład w przypadku wykrycia luk, które wymagają zmian w aplikacjach.

2) Ocena instancji portfela powinna uwzględniać te szczególne wyzwania. Jedną z bezpośrednich konsekwencji jest to, że ramy wspólnych kryteriów mogą nie być odpowiednie we wszystkich przypadkach. W związku z tym, w razie potrzeby, należy rozważyć alternatywne metody oceny. Krajowe programy certyfikacji uwzględniają zastosowanie metodologii określonej w normie EN 17640:2018 w następujących przypadkach:

a) w ramach samego systemu;

b) za pośrednictwem systemów krajowych opartych na tej metodyce;

c) za pośrednictwem systemów krajowych opartych na podobnych zasadach, lecz utworzonych przed opracowaniem metodologii określonej w normie EN 17640:2018.

3) Ponadto, z uwagi na ograniczoną wartość dodaną przeprowadzania pełnej, specjalnej oceny każdego wariantu, krajowe programy certyfikacji muszą uwzględniać określenie kryteriów umożliwiających przeprowadzenie doboru próby, aby uniknąć powtarzania tych samych działań w zakresie oceny i móc się skupić na działaniach charakterystycznych dla danego wariantu. Krajowe programy certyfikacji wymagają od wszystkich jednostek certyfikujących uzasadnienia stosowania przez nie doboru próby.

4) Krajowe programy certyfikacji obejmują aktualizacje instancji portfela w ogólnym procesie zarządzania zmianami określonym dla rozwiązania w zakresie portfela. Wskazują również zasady dotyczące procedur, które mają być stosowane przez dostawcę portfela w odniesieniu do każdej aktualizacji (np. analizy wpływu zmian na środki kontroli w zakresie ochrony), oraz dotyczące działań w zakresie oceny, które jednostka certyfikująca przeprowadza w odniesieniu do aktualizacji w określonych warunkach (np. oceny skuteczności operacyjnej zmodyfikowanej kontroli bezpieczeństwa). Proces zarządzania zmianami jest jednym z procesów, których skuteczność operacyjna podlega corocznej kontroli zgodnie z art. 18 ust. 3.

6. **Działania w zakresie oceny dotyczące usług i procesów wykorzystywanych w celu zapewniania i obsługi rozwiązania w zakresie portfela**

1) Na potrzeby oceny usług i procesów, które odgrywają rolę w zapewnianiu i obsłudze rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, zespół ds. oceny gromadzi dowody w drodze działań w zakresie oceny, które mogą obejmować działania w zakresie kontroli, inspekcji, weryfikacji i walidacji.

2) Jednostka certyfikująca ma obowiązek potwierdzić, że dowody są wystarczające i odpowiednie do zapewnienia należytej pewności, że usługi i procesy spełniają wymogi certyfikacji, poprzez sprawdzenie następujących elementów:

   a) dokładności informacji przedstawionych w opisie procesów i usług;

   b) adekwatności projektu oraz mechanizmów kontrolnych procesów i usług w kontekście spełnienia kryteriów oceny;

   c) skuteczności operacyjnego wdrożenia kontroli w określonym okresie poprzedzającym ocenę.

3) Dokładność opisu i skuteczność operacyjną wdrożenia kontroli można uznać za cele weryfikacji zgodnie z normą ISO/IEC 17000:2020 w odniesieniu do odpowiednich oświadczeń dostawcy portfela (tj. potwierdzenie rzetelności zdarzeń, które już wystąpiły, lub już uzyskanych wyników), natomiast przydatność projektu i kontroli usług i procesów do spełnienia kryteriów oceny można uznać za cel walidacji zgodnie z normą ISO/IEC 17000:2020 w odniesieniu do odpowiedniego oświadczenia dostawcy portfela (tj. potwierdzenie wiarygodności w kontekście planowanego przyszłego wykorzystania lub przewidywanego wyniku).

4) Biorąc pod uwagę, że rozwiązanie w zakresie portfela nie jest dopuszczone do użytku przed certyfikacją, skuteczność operacyjna nie może być zweryfikowana na podstawie jego faktycznego funkcjonowania. W związku z tym należy to potwierdzić za pomocą dowodów zgromadzonych podczas testów lub badań pilotażowych.

5) Krajowe programy certyfikacji mogą już istnieć w odniesieniu do konkretnych usług i procesów, na przykład w zakresie rejestracji użytkowników. W stosownych przypadkach krajowe programy certyfikacji powinny rozważyć zastosowanie takich programów.

7. **Działania w zakresie oceny dotyczące usług ICT wykorzystywanych do zapewniania i obsługi rozwiązania w zakresie portfela**

1) Niektóre architektury portfela mogą polegać na specjalnych usługach ICT, takich jak usługi w chmurze, które wspierają zapewnianie i obsługę rozwiązania w zakresie portfela, przy czym te usługi ICT mogą przechowywać dane wrażliwe oraz wykonywać operacje wrażliwe. W takim przypadku krajowe programy certyfikacji muszą określić wymogi bezpieczeństwa dla takich usług ICT.

2) Istnieje już wiele programów certyfikacji usług ICT, usług w chmurze i innych źródeł informacji na temat bezpieczeństwa, łącznie z tymi wymienionymi w załączniku II. Krajowe programy certyfikacji, jeśli są dostępne i mają zastosowanie, powinny korzystać z istniejących metod za pośrednictwem jednego z następujących mechanizmów:

   a) upoważnienie do korzystania z konkretnego programu lub wybranych programów poprzez określenie warunków, na jakich usługi ICT lub usługi w chmurze mają być oceniane za pomocą takich systemów;

   b) pozostawienie wyboru sposobu oceny dostawcy portfela oraz zastosowanie analizy zależności w celu oceny adekwatności informacji na temat bezpieczeństwa uzyskanych na podstawie tych ocen.

3) W obu przypadkach krajowe programy certyfikacji określają dodatkowe działania w zakresie oceny niezbędne do przeanalizowania lub uzupełnienia informacji uzyskanych w ramach tych programów.

ZAŁĄCZNIK V

WYKAZ PUBLICZNIE DOSTĘPNYCH INFORMACJI NA TEMAT PORTFELI

1. Informacje podawane do wiadomości publicznej zgodnie z art. 8 ust. 5 muszą obejmować co najmniej:
   a) wszelkie ograniczenia dotyczące stosowania rozwiązania w zakresie portfela;
   b) wytyczne i zalecenia opracowane przez dostawcę portfela, aby pomóc użytkownikom końcowym w bezpiecznej konfiguracji, instalacji, wdrażaniu, eksploatacji i utrzymaniu portfeli;
   c) okres, w którym użytkownikom końcowym oferowane jest wsparcie w zakresie bezpieczeństwa, w szczególności pod względem dostępności aktualizacji związanych z cyberbezpieczeństwem;
   d) dane kontaktowe producenta lub dostawcy oraz akceptowane sposoby otrzymywania informacji o podatności na zagrożenia pochodzących od użytkowników końcowych i ekspertów w obszarze bezpieczeństwa;
   e) odniesienie do repozytoriów internetowych zawierających wykaz publicznie ujawnionych podatności w obszarze portfeli oraz do wszelkich odpowiednich doradców ds. cyberbezpieczeństwa.

2. Informacje, o których mowa w ust. 1, należy udostępnić każdej osobie, która chciałaby skorzystać z rozwiązania w zakresie portfela, w sposób jasny, wyczerpujący i przystępny, w ogólnodostępnej przestrzeni.

ZAŁĄCZNIK VI

METODYKA OCENY DOPUSZCZALNOŚCI INFORMACJI NA TEMAT BEZPIECZEŃSTWA

1. **Ocena dostępności dokumentacji bezpieczeństwa**

Oceniający mają obowiązek przedstawić dokumentację bezpieczeństwa dostępną w odniesieniu do każdego istotnego komponentu rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane. Następnie oceniający oceniają ogólne znaczenie każdego dokumentu dotyczącego bezpieczeństwa dla przeglądu zależności.

W analizie uwzględnia się następujące elementy:

1) informacje na temat samej dokumentacji bezpieczeństwa:

   a) rodzaj dokumentacji bezpieczeństwa wraz ze wszystkimi wymaganymi szczegółami

      (przykładami takich dokumentów są certyfikaty zgodności zgodnie z normą EN ISO/IEC 27001:2022 lub typ 1 lub 2 dla sprawozdań ISAE);

   b) badany okres lub okres ważności

      (okres ten może zostać uzupełniony o pismo pomostowe (dokument obejmujący okres między datą zakończenia okresu sprawozdawczego bieżącego sprawozdania ISAE a opublikowaniem nowego sprawozdania ISAE) lub podobne oświadczenie);

   c) właściwe ramy (np. istniejąca norma);

   d) czy dokumentacja bezpieczeństwa zawiera przyporządkowanie do wymogów systemu;

2) kompetencje zawodowe i bezstronność wydawcy sprawozdania dotyczącego bezpieczeństwa:

   a) nazwa jednostki certyfikującej oraz, jeśli jest dostępna, nazwa wiodącego oceniającego;

   b) dowody potwierdzające kompetencje jednostki certyfikującej i oceniającego (np. akredytacja, certyfikacja osobista itp.);

   c) dowód bezstronności jednostki certyfikującej i oceniającego (np. akredytacja itp.).

2. **Ocena bezpieczeństwa w odniesieniu do indywidualnych wymogów**

Oceniający sprawdzają, czy dokumentacja bezpieczeństwa dostępna dla rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, nadaje się do ustalenia, czy rozwiązanie w zakresie portfela spełnia oczekiwania w zakresie indywidualnych wymogów programu certyfikacji.

Ocenę tę przeprowadza się w odniesieniu do każdego istotnego komponentu rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, poprzez sformułowanie założenia dotyczącego kontroli bezpieczeństwa stosowanych w rozwiązaniu w zakresie portfela.

W odniesieniu do każdego takiego założenia zespół ds. oceny ustala, czy poziom bezpieczeństwa określony w dostępnej dokumentacji bezpieczeństwa jest odpowiedni.

Stwierdzenie, że poziom bezpieczeństwa jest właściwy, musi się opierać na następujących podstawach:

1) wymagane informacje są dostępne, wraz z oczekiwanym poziomem bezpieczeństwa, w dokumentacji bezpieczeństwa;

2) informacje dostępne w dokumentacji bezpieczeństwa nie obejmują pełnego zakresu wymogu, ale dodatkowe kontrole lub kontrole kompensacyjne (tj. kontrole wewnętrzne, które zmniejszają ryzyko wystąpienia istniejących lub potencjalnych niedociągnięć w zakresie kontroli) wdrożone w rozwiązaniu w zakresie portfela lub systemie identyfikacji elektronicznej, w ramach którego są ono są one zapewniane, umożliwiają oceniającym ustalenie, czy informacje te są odpowiednie;

3) informacje dostępne w dokumentacji bezpieczeństwa nie zapewniają oczekiwanego poziomu bezpieczeństwa, ale kontrole przeprowadzone w celu oceny i monitorowania dostawcy portfela umożliwiają oceniającym ustalenie, czy informacje te są odpowiednie;

4) jeżeli w dokumentacji bezpieczeństwa wskazano niezgodności dotyczące projektu lub wdrożenia kontroli wykorzystywanych do spełnienia założenia, działania naprawcze zaproponowane i wdrożone przez dostawcę portfela i poddane przeglądowi przez jego oceniających muszą być odpowiednie, aby zagwarantować, że założenie zostało rzeczywiście spełnione.

ZAŁĄCZNIK VII

TREŚĆ CERTYFIKATU ZGODNOŚCI

1. Niepowtarzalny identyfikator nadany przez jednostkę certyfikującą wydającą certyfikat zgodności.

2. Informacje dotyczące certyfikowanego rozwiązania w zakresie portfela oraz systemów identyfikacji elektronicznej, w ramach których są one zapewniane, oraz informacje na temat posiadacza certyfikatu zgodności, w tym:
   a) nazwa rozwiązania w zakresie portfela;
   b) nazwy systemów identyfikacji elektronicznej, w ramach których zapewnia się rozwiązanie w zakresie portfela;
   c) wersja rozwiązania w zakresie portfela, która została poddana ocenie;
   d) imię i nazwisko lub nazwa, adres i dane kontaktowe posiadacza certyfikatu zgodności;
   e) link do strony internetowej posiadacza certyfikatu zgodności zawierającej informacje, które muszą być udostępnione publicznie.

3. Informacje dotyczące oceny i certyfikacji rozwiązania w zakresie portfela oraz systemów identyfikacji elektronicznej, w ramach których są one zapewniane, w tym:
   a) nazwa, adres i dane kontaktowe jednostki certyfikującej, która wydała certyfikat zgodności;
   b) w przypadku gdy jednostka oceniająca zgodność jest inna niż jednostka certyfikująca – nazwa jednostki oceniającej zgodność, która dokonała oceny, wraz z informacjami na temat jej akredytacji;
   c) imię i nazwisko lub nazwa właściciela programu;
   d) odniesienia do rozporządzenia (UE) nr 910/2014 i do niniejszego rozporządzenia;
   e) odniesienie do raportu z certyfikacji związanego z certyfikatem zgodności;
   f) odniesienie do sprawozdania z oceny certyfikacji związanej z certyfikatem zgodności;
   g) odniesienie do norm stosowanych w przypadku dokonywania oceny, łącznie z ich wersjami;
   h) data wydania certyfikatu zgodności;
   i) okres ważności certyfikatu zgodności.

ZAŁĄCZNIK VIII

TREŚĆ PUBLICZNEGO RAPORTU Z CERTYFIKACJI I SPRAWOZDANIA Z OCENY CERTYFIKACJI

1. Publiczny raport z certyfikacji musi obejmować co najmniej następujące elementy:

   a) streszczenie;

   b) identyfikację rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane;

   c) opis rozwiązania w zakresie portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one zapewniane;

   d) informacje dotyczące bezpieczeństwa, które mają być podawane do wiadomości publicznej, zgodnie z opisem w załączniku V, lub odnośnik do tych informacji;

   e) streszczenie wstępnego planu kontroli i walidacji;

   f) streszczenie decyzji w sprawie przeglądu i certyfikacji.

2. Sprawozdanie z oceny certyfikacji musi zawierać co najmniej:

   a) opis projektu rozwiązania w zakresie portfela, systemu identyfikacji i procesu rejestracji wraz z oceną ryzyka i szczegółowym planem walidacji;

   b) opis tego, w jaki sposób rozwiązanie w zakresie portfela spełnia wymogi wysokiego poziomu bezpieczeństwa oraz w jaki sposób wykazano to na podstawie wyników oceny certyfikacji rozwiązania w zakresie portfela przeprowadzonej zgodnie z niniejszym rozporządzeniem;

   c) opis wyniku oceny zgodności rozwiązania w zakresie portfela i systemu identyfikacji elektronicznej, w ramach którego są dostarczane odpowiednie jednostki portfela, w szczególności zgodność z:

      — wymogami określonymi w art. 5a ust. 4, 5 i 8 rozporządzenia (UE) nr 910/2014;

      — wymogiem logicznego oddzielenia określonym w art. 5a ust. 14 rozporządzenia (UE) nr 910/2014;

      — w stosownych przypadkach, normami i specyfikacjami technicznymi, o których mowa w art. 5a ust. 24 rozporządzenia (UE) nr 910/2014, przy jednoczesnym opisaniu, w jaki sposób wymogi te odnoszą się do odpowiednich wymogów normatywnych określonych przez krajowe programy certyfikacji;

   d) podsumowanie wyników realizacji planu walidacji, w tym wszystkich stwierdzonych niezgodności.

ZAŁĄCZNIK IX

HARMONOGRAM OBOWIĄZKOWYCH OCEN NADZORU

1. W art. 18 określono wymogi dotyczące cyklu życia certyfikacji, w szczególności przeprowadzania regularnych działań w zakresie oceny. Czynności te muszą obejmować co najmniej:

   a) pełną ocenę przedmiotu oceny zgodności w ramach oceny wstępnej i przy każdej ponownej ocenie certyfikacji, w tym aktualizację komponentów produktu;

   b) ocenę podatności na zagrożenia w ramach oceny wstępnej i przy każdej ponownej ocenie certyfikacji oraz co najmniej raz na dwa lata w ramach ocen nadzoru, obejmującą przynajmniej zmiany przedmiotu oceny zgodności i zmiany w środowisku zagrożenia od czasu ostatniej oceny podatności na zagrożenia;

   c) dodatkowe działania, takie jak testy penetracyjne w przypadku podwyższonego poziomu ryzyka lub pojawienia się nowych zagrożeń;

   d) ocenę skuteczności operacyjnej procesów utrzymania co najmniej raz w roku w ramach oceny nadzoru i ponownej certyfikacji, obejmującą przynajmniej procesy kontroli wersji, aktualizacji i zarządzania podatnością;

   e) po pozytywnej decyzji w sprawie przeglądu i certyfikacji – wydanie certyfikatu zgodności po przeprowadzeniu wstępnej oceny i po każdej ponownej ocenie certyfikacji.

2. Harmonogram referencyjny wskazano w tabeli 1 w oparciu o cykl czteroletni, w którym:

   a) rok 1 rozpoczyna się z chwilą wydania certyfikatu zgodności po raz pierwszy; oraz

   b) wszystkie działania w zakresie oceny przeprowadza się w ciągu 12 miesięcy od oceny z poprzedniego roku.

3. Harmonogram przedstawiony w tabeli 1 stanowi zalecenie mające na celu zapewnienie terminowej ponownej certyfikacji i uniknięcie zakłóceń w dostarczaniu rozwiązania w zakresie portfela. Dopuszcza się inne harmonogramy, o ile ważność certyfikatu zgodności nie przekracza pięciu lat, jak określono w art. 5c ust. 4 rozporządzenia (UE) nr 910/2014.

4. Oprócz regularnych ocen na żądanie jednostki certyfikującej lub posiadacza certyfikatu zgodności może zostać przeprowadzona specjalna ocena w następstwie istotnej zmiany przedmiotu certyfikacji lub środowiska zagrożenia.

5. Każda ocena, w tym oceny nadzoru i oceny specjalne, może prowadzić do wydania nowego certyfikatu zgodności, w szczególności w przypadku istotnych zmian przedmiotu certyfikacji, ale z taką samą datą wygaśnięcia co pierwotny certyfikat zgodności.

Tabela 1

Pełny czteroletni cykl oceny

Czas	Rodzaj oceny	Czynności
Rok 0	Wstępna	— Pełna ocena przedmiotu certyfikacji, w tym ocena podatności na zagrożenia — W tym funkcja służąca do aktualizacji każdego komponentu oprogramowania — Ocena procesów utrzymania, z wyłączeniem ich skuteczności operacyjnej — Wydanie certyfikatu zgodności i rozpoczęcie cyklu czteroletniego
Rok 1	Nadzór	— Ocena skuteczności operacyjnej procesów utrzymania — Co najmniej sprawdzenie wersji, aktualizacja, zarządzanie podatnością na zagrożenia — Ocena zmian mających wpływ na bezpieczeństwo produktu

Czas	Rodzaj oceny	Czynności
Rok 2	Nadzór	— Ocena podatności na zagrożenia pełnego rozwiązania — Ocena skuteczności operacyjnej procesów utrzymania — — Co najmniej kontrola wersji, aktualizacja, zarządzanie podatnością na zagrożenia — Ocena zmian mających wpływ na bezpieczeństwo produktu
Rok 3	Nadzór	— Ocena skuteczności operacyjnej procesów utrzymania — — Co najmniej sprawdzenie wersji, aktualizacja, zarządzanie podatnością na zagrożenia — Ocena zmian mających wpływ na bezpieczeństwo produktu
Rok 4	Ponowna certyfikacja	(1) Pełna ocena przedmiotu certyfikacji, w tym ocena podatności na zagrożenia (2) Uproszczona ocena elementów/procesów, które pozostały niezmienione (3) W tym funkcja służąca do aktualizacji każdego komponentu oprogramowania (4) Ocena procesów utrzymania, w tym ich skuteczności operacyjnej (5) Wydanie nowego świadectwa zgodności