

G-01

System Certyfikacji PL Portfela EUDI

Wersja 1.01

2026.07.09

Oznaczenie dokumentu	G-01
Wersja	1.01
Status	Final
Data	09.07.2026
Rodzaj dokumentu	Dokument ramowy
Ramy nadrzędne	brak
Właściciel programu	Rzeczpospolita Polska / Minister Cyfryzacji
Przedmiot certyfikacji	Rozwiązanie Portfela EUDI
Odbiorcy pierwotni	Właściciel systemu/programu, jednostki CAB, dostawca Portfela EUDI, dostawca PID
Odbiorcy wtórni	Interesariusze ekosystemu Portfela EUDI
Poziom uzasadnienia zaufania <potwierdzenie tożsamości, CIR 2015/1502> lub <ocena, rozporządzenie (UE) 2019/881>	Wysoki/Wysoki
Dokumenty podrzędne	dokumenty GP-01, GP-02, GP-03 (programy certyfikacji) serie dokumentów WZ, WP, WM

Historia zmian

Nr.	Zmiana	Wersja	Data
1.	Tłumaczenie wersji angielskiej	1.0	2026-06-15
2.	Rozdział 5 rozszerzony o (nowe) sekcje: 5.1, 5.3 (przeniesiona z GP-03), 5.5 i 5.7; zaktualizowano Rysunek 3; Zmiany edycyjne	1.01	2026-07-09

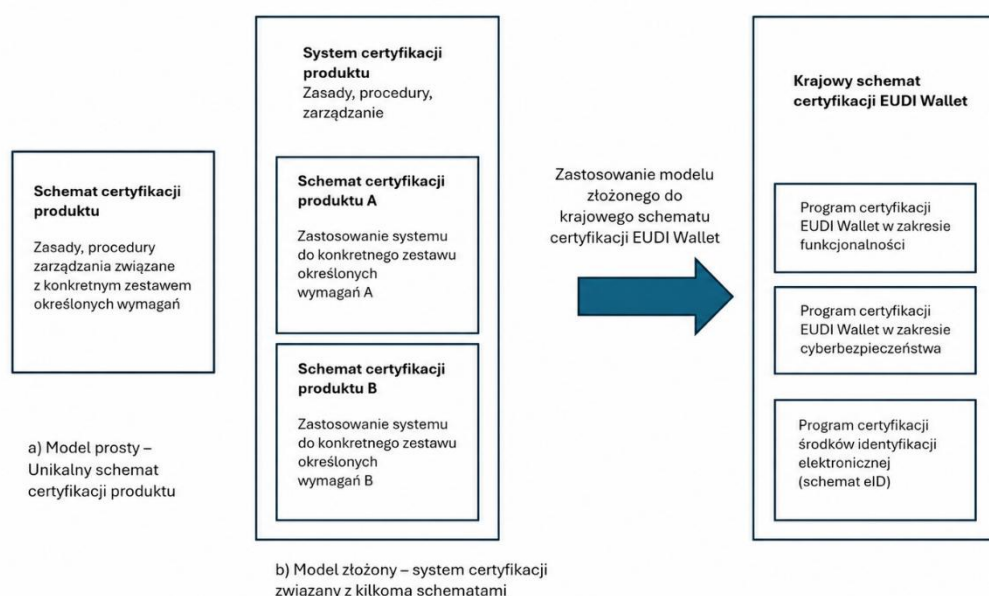
Spis treści

1	WPROWADZENIE	6
2	DOKUMENTY PRAWNE I NORMATYWNE	9
3	ŁAD ORGANIZACYJNY I RELACJE INTERESARIUSZY	10
3.1	Interesariusze	10
3.1.1	Właściciel systemu.....	10
3.1.2	Właściciel programu.....	10
3.1.3	Krajowa jednostka akredytująca (NAB)	11
3.1.4	Jednostka oceniająca zgodność (CAB-CB)	11
3.1.5	Jednostka oceniająca zgodność (CAB-ITSEF)	11
3.1.6	Wnioskodawca / Posiadacz certyfikatu	11
3.2	Współpraca transgraniczna i nadzór.....	12
3.2.1	Europejska Grupa Współpracy ds. Tożsamości Cyfrowej (EDICG).....	12
3.2.2	Organ nadzoru (SA)	12
4	OBOWIĄZKOWE ELEMENTY DEFINICJI PROGRAMU NA PODSTAWIE PN-EN ISO/IEC 17067	13
4.1	Własność programu.....	13
4.2	Zakres i cele	15
4.3	Elementy programu według PN-EN ISO/IEC 17067	18
5	ZARZĄDZANIE CYKLEM ŻYCIA PROGRAMU	22
5.1	Warunki uczestnictwa CAB w programie certyfikacji	22
5.2	Ogólne zasady dotyczące procesu certyfikacji.....	22
5.3	Dowody uzasadnienia zaufania ze źródeł zewnętrznych.....	23
5.4	Nadzór.....	23
5.5	Obowiązki posiadaczy certyfikatów po certyfikacji.....	24
5.6	Zmiany przedmiotu certyfikacji najwyższego poziomu.....	25
5.7	Postępowanie z niezgodnościami	26
5.8	Zawieszenie, rozwiązanie, cofnięcie lub wygaśnięcie certyfikatów	27
5.9	Skargi i odwołania.....	28
5.10	Przechowywanie zapisów	29
5.11	Okresowy przegląd programu certyfikacji	29
5.12	Utrzymanie programu	29
5.13	Przegląd wzajemny.....	30
6	PRZEGLĄD METOD OCENY ZGODNOŚCI, SPECYFIKACJI I RAPORTOWANIA	31

6.1	Postanowienia ogólne	31
6.2	Elementy wymagane do zdefiniowania w ramach metod oceny zgodności	31
6.3	Obowiązkowe elementy raportów	31
6.4	Szablon oceny zgodności dedykowany programom certyfikacji	33
7	ANALIZA ZGODNOŚCI	35
7.1	Zgodność z rozporządzeniem eIDAS i właściwymi aktami wykonawczymi	35
7.1.1	Zgodność z aktem wykonawczym (CIR (UE) 2024/2981)	35
7.2	Zgodność z Aktem o cyberbezpieczeństwie (UE) (art. 54 ust. 1 – Elementy europejskich programów certyfikacji cyberbezpieczeństwa	43
	ZAŁĄCZNIK A METODY I TECHNIKI OCENY ZGODNOŚCI	48
A.1.	Terminy dotyczące oceny zgodności	48
A.2.	Metody dotyczące oceny	48
A.3.	Różne rodzaje atestacji	49
	ZAŁĄCZNIK B OPIS ARCHITEKTURY ROZWIĄZANIA PORTFELA W POLSCE	51

1 Wprowadzenie

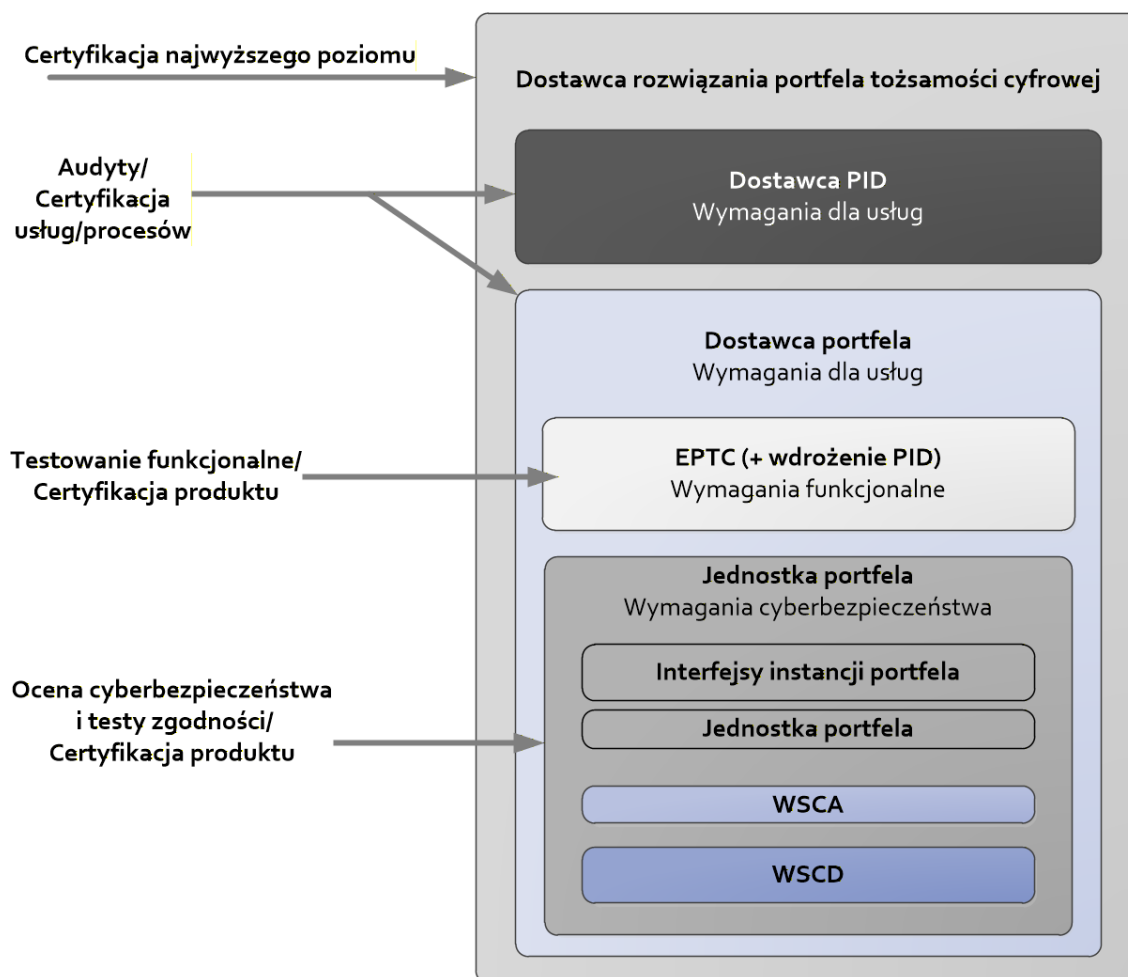
- 1 Niniejszy dokument stanowi ramy wysokiego poziomu objaśniające system certyfikacji Portfela EUDI, zapewniając jego zgodność z powiązanymi regulacjami.
- 2 System certyfikacji opiera się na koncepcji i treści systemu certyfikacji opisanego w PN-EN ISO/IEC 17067 (zob. Rysunek 1.)



Rysunek 1 Koncepcja systemu certyfikacji zastosowana do krajowych programów certyfikacji Portfela EUDI

- 3 *UWAGA 1: Używane pojęcia „portfel EUDI”, „europejski portfel tożsamości cyfrowej” wraz ze skrótem „EPTC” są synonimami*
- 4 *UWAGA 2: Zgodnie z PN-EN ISO/IEC 17000 terminy „scheme” (program) i „program” są synonimami.*
- 5 System Certyfikacji PL Portfela EUDI ma na celu dostarczenie Komisji Europejskiej i EDICG informacji o certyfikowanym rozwiązaniu portfela tożsamości cyfrowej (certyfikat najwyższego poziomu (Rysunek 2), zgodnie z art. 5d ust. 1 rozporządzenia (UE) 910/2014, na podstawie zbioru certyfikatów lub deklaracji zgodności wynikających z realizacji wszystkich właściwych programów certyfikacji.

- 6 Wszystkie certyfikaty bazowe wskazane na rysunku (Rysunek 2) oraz bazowe programy certyfikacji muszą być zgodne z PN-EN ISO/IEC 17067 i PN-EN ISO/IEC 17065, jednak nie mają one szczególnego statusu na gruncie rozporządzenia wykonawczego Komisji (UE) 2024/2981 dotyczącego certyfikacji europejskich portfeli tożsamości cyfrowej (zob. Rozporządzenie (UE) 910/2014, art. 5c ust. 6).



Rysunek 2 Zbiór certyfikatów/deklaracji zgodności wynikających z realizacji krajowego systemu certyfikacji Portfela EUDI

- 7 Rysunek ilustruje strukturalną kompozycję systemu certyfikacji Portfela EUDI, pokazując, w jaki sposób poszczególne programy certyfikacji – funkcjonalny, cyberbezpieczeństwa i eID – łączą się, tworząc całościowy certyfikat dostawcy Portfela EUDI.
- 8 Wizualnie diagram zorganizowany jest jako warstwowa, modułowa architektura.

(a) Na dole:

- o podsystem certyfikacji typu produktowego składa się z co najmniej dwóch odrębnych zewnętrznych komponentów certyfikacji cyberbezpieczeństwa, tj. certyfikatu WSCA i certyfikatu WSCD, obu realizowanych według programu cyberbezpieczeństwa EUCC, oraz oceny cyberbezpieczeństwa instancji portfela i jednostki portfela (jako całości), według programu opartego na EN17640:2022 + A1:2026. Program certyfikacji typu produktowego zdefiniowany w GP-02 jest dedykowany produktowi reprezentowanemu jako **złożony TOE**.

(b) W środku:

- o Blok certyfikacji funkcjonalnej reprezentuje zbiór działań oceny zgodności (funkcjonalny program certyfikacji) dotyczących funkcjonalności portfela, procesów onboardingu, wydawania PID oraz zachowania na poziomie usług.
- o Program certyfikacji typu usługowego odnosi się do wymagań bezpieczeństwa (technicznych i organizacyjnych) dotyczących usług świadczonych przez dostawcę PID i dostawcę Portfela EUDI.

(c) Na górze:

- o Blok certyfikacji systemu eID odzwierciedla wymagania związane z usługami systemu identyfikacji, poziomami uzasadnienia zaufania (w rozumieniu CIR 2015/1502) oraz zgodnością dostawcy PID i dostawcy Portfela EUDI, zgodnie z wymogami ram prawnych.

9 Ogólnie rysunek pokazuje, w jaki sposób system certyfikacji został zaprojektowany jako model złożony, w którym kilka niezależnych, lecz wzajemnie powiązanych programów certyfikacji przyczynia się do zharmonizowanego i interoperacyjnego wyniku certyfikacji europejskiego portfela tożsamości cyfrowej.

2 Dokumenty prawne i normatywne

- 10 W celu przeprowadzania certyfikacji europejskich portfeli tożsamości cyfrowej ustanawia się system certyfikacji w zakresie zgodności z rozporządzeniem (UE) 910/2014, na podstawie norm PN-EN ISO/IEC 17067 i PN-EN ISO/IEC 17065, funkcjonujący w ramach systemu oceny zgodności opisanego w rozporządzeniu 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.
- 11 Program certyfikacji Portfela EUDI oraz jego programy wykazują zgodność z następującymi dokumentami:
- (a) Ramy funkcjonalne rozporządzenia 910/2014 (art. 5a) oraz właściwe rozporządzenia wykonawcze Komisji :
 - o EU 2024/2977
 - o EU 2024/2979
 - o EU 2024/2982
 - (b) Zasady certyfikacji (art. 5c rozporządzenia (UE) 910/2014) oraz rozporządzenie (UE) 2024/2981
 - (c) Europejski program certyfikacji cyberbezpieczeństwa EUCC, zdefiniowany w rozporządzeniu wykonawczym Komisji (UE) 2024/482
 - (d) Art. 54 rozporządzenia UE 2019/881 (Akt o cyberbezpieczeństwie)
 - (e) Art. 8 ust. 3 rozporządzenia UE 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych wraz z rozporządzeniem wykonawczym Komisji (UE) 2015/1502
 - (f) Rozporządzenie (UE) 765/2008 ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu (..), w szczególności art. 4 i 5
 - (g) Ustawa z dnia 24 września 2010 r. o ewidencji ludności
 - (h) Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych
 - (i) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 lutego 2019 r. w sprawie warstwy elektronicznej dowodu osobistego

- (j) Rozporządzenie Ministra Cyfryzacji z dnia 15 października 2021 r. w sprawie prowadzenia Rejestru Dowodów Osobistych
- (k) Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej
- (l) Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel
- (m) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
- (n) Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach

3 Ład organizacyjny i relacje interesariuszy

3.1 Interesariusze

12 Niniejsza sekcja krótko opisuje interesariuszy zaangażowanych w System Certyfikacji Portfela EUDI, ich role i obowiązki.

3.1.1 Właściciel systemu

13 **Rola:** Organ zarządzający najwyższego szczebla systemu certyfikacji.

14 **Obowiązki:**

- o Definiowanie zasad systemu certyfikacji.
- o Utrzymywanie i aktualizowanie dokumentacji systemu.
- o Zapewnianie zgodności całego systemu z PN-EN ISO/IEC 17067.

3.1.2 Właściciel programu

15 **Rola:** Zarządzanie każdym programem certyfikacji

16 **Obowiązki:**

- o Definiowanie szczegółowych zasad dotyczących programu
- o Utrzymywanie dokumentacji właściwej dla programu
- o Zapewnianie zgodności z wymaganiami PN-EN ISO/IEC 17067 na poziomie programu.
- o Nadzór nad działaniami certyfikacyjnymi
- o Zgodność certyfikowanych rozwiązań z krajowymi i unijnymi ramami prawnymi
- o Monitorowanie po certyfikacji, w szczególności w następstwie incydentów lub podatności

17 *UWAGA: Role Właściciela systemu i Właściciela programu mogą być łączone.*

3.1.3 Krajowa jednostka akredytująca (NAB)

18 **Rola:** Zapewnia zaufanie i kompetencje jednostek oceniających zgodność (CAB).

19 **Obowiązki:**

- o Akredytacja CAB-CB zgodnie z PN-EN ISO/IEC 17065 lub innymi normami, jeżeli wymaga tego program
- o Akredytacja CAB-ITSEF zgodnie z PN-EN ISO/IEC 17025, we właściwych programach certyfikacji
- o Weryfikacja kompetencji, bezstronności i spójnego stosowania zasad certyfikacji
- o Działanie w ramach nadrzędnych unijnych ram akredytacji (rozporządzenie 765/2008) oraz właściwych polskich aktów prawnych.

3.1.4 Jednostka oceniająca zgodność (CAB-CB)

20 **Rola:** Wykonuje działania oceny zgodności lub zleca je podwykonawcom.

21 **Obowiązki:**

- o Przeprowadzanie lub podzlecanie ocen, audytów lub badań
- o Sporządzanie lub walidacja raportów z badań, raportów z oceny oraz dokumentacji certyfikacyjnej
- o Wspieranie procesu decyzyjnego w zakresie ustaleń dotyczących zgodności.

3.1.5 Jednostka oceniająca zgodność (CAB-ITSEF)

22 **Rola:** Wykonuje działania oceny lub badań.

23 **Obowiązki:**

- o Przeprowadzanie ocen lub badań
- o Sporządzanie raportów z badań, raportów z oceny oraz dokumentacji oceny
- o Wspieranie procesu decyzyjnego CAB-CB w zakresie ustaleń dotyczących zgodności.

3.1.6 Wnioskodawca / Posiadacz certyfikatu

24 **Rola:** Podmiot ubiegający się o certyfikację lub posiadający certyfikat. Zwykle jest to dostawca Portfela EUDI lub dostawca PID.

25

Obowiązki:

- o Złożenie wniosku o certyfikację
- o Dostarczenie całej wymaganej dokumentacji technicznej, proceduralnej i dotyczącej bezpieczeństwa
- o Ciągłe utrzymywanie zgodności w całym okresie funkcjonowania (w tym obowiązki po certyfikacji).

3.2

Współpraca transgraniczna i nadzór

26

W kontekście współpracy transgranicznej mogą zostać ustanowione dwie dodatkowe role.

3.2.1

Grupa Współpracy na rzecz Europejskiej Tożsamości Cyfrowej (EDICG)

27

Rola: Koordynacja i harmonizacja europejskich ram tożsamości cyfrowej na poziomie UE

28

Obowiązki:

- o Wspieranie spójnego wdrażania ram Portfela EUDI we wszystkich państwach członkowskich.
- o Ułatwianie współpracy między organami krajowymi, w tym w zakresie nadzoru, obsługi incydentów i interoperacyjności transgranicznej.
- o Zapewnianie wytycznych w celu jednolitego stosowania wymagań związanych z certyfikacją.
- o Wspomaganie Komisji Europejskiej w monitorowaniu i doskonaleniu funkcjonowania europejskiego ekosystemu tożsamości cyfrowej.

3.2.2

Organ nadzoru (SA)

29

UWAGA: Rola SA nie może być łączona z rolą Właściciela systemu/programu. Do tych ról zostały wyznaczone różne komórki organizacyjne Ministerstwa Cyfryzacji.

30

Rola: Funkcja nadzorcza i kontrolna

31

Obowiązki:

- o Nadzór nad ramami zaufania (zob. G-03)
- o Współpraca transgraniczna i procesy notyfikacji.

4 Obowiązkowe elementy definicji programu na podstawie PN-EN ISO/IEC 17067

4.1 Własność programu

32 *UWAGA: tekst dotyczy obu ról: Właściciela systemu i Właściciela programu.*

33 Zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2981, rozdział II, art. 3 ust. 1 dotyczącym ustanawiania krajowych programów certyfikacji, państwa członkowskie wyznaczają Właściciela programu dla każdego krajowego systemu certyfikacji.

34 Właścicielem krajowego systemu certyfikacji portfela EUDI jest Minister Cyfryzacji.

35 Właściciel programu:

- (a) przyjmuje pełną odpowiedzialność za cele, treść i integralność programu;
- (b) utrzymuje program i zapewnia wytyczne, gdy jest to wymagane;
- (c) ustanawia strukturę do prowadzenia programu i zarządzania nim;
- (d) dokumentuje treść programu;
- (e) zapewnia, aby program był opracowywany przez osoby kompetentne zarówno w aspektach technicznych, jak i oceny zgodności;
- (f) planuje ochronę poufności informacji przekazywanych przez strony zaangażowane w program;
- (g) prowadzi i utrzymuje rejestr ryzyk zdefiniowany w CIR (UE) 2024/2981;
- (h) ocenia ryzyka/zobowiązania wynikające z jego działalności i zarządza nimi;
- (i) zatwierdza zakres działań podzlecanych przez jednostkę certyfikującą;

36 Właściciel programu może zlecić podwykonawstwo określonej części swoich zadań stronie trzeciej. Podzlecając zadania stronie trzeciej, Właściciel programu określa w umowie obowiązki i zakres odpowiedzialności wszystkich stron. Właściciele programów pozostają odpowiedzialni za wszystkie podzleczone działania wykonywane przez ich podwykonawców.

- 37 Właściciel programu publikuje listę certyfikowanych rozwiązań Portfela EUDI wraz z informacjami określonymi w załączniku V do CIR (UE) 2024/2981.
- 38 Właściciel programu monitoruje zgodność CAB-CB z ich obowiązkami wynikającymi z rozporządzenia (UE) nr 910/2014 oraz z krajowych programów certyfikacji.
- 39 Właściciel programu prowadzi działania monitorujące, w stosownych przypadkach, co najmniej na podstawie następujących informacji:
- (a) informacji pochodzących od jednostek certyfikujących (CAB-CB), laboratoriów badawczych (CAB-ITSEF), krajowych jednostek akredytujących oraz właściwych organów nadzoru rynku, w stosownych przypadkach;
 - (b) informacji wynikających z audytów i postępowań wyjaśniających własnych lub innego organu;
 - (c) skarg i odwołań otrzymanych zgodnie z pkt 40.
- 40 Właściciel programu zarządza programem w całym jego cyklu życia oraz posiada procedury przeglądu i doskonalenia programu na podstawie:
- (a) informacji zebranych od interesariuszy ekosystemu Portfela EUDI, w tym między innymi od CAB, dostawców portfeli, innych państw członkowskich oraz Grupy Współpracy na rzecz Europejskiej Tożsamości Cyfrowej;
 - (b) własnych działań monitorujących;
 - (c) procesów skarg i odwołań;
 - (d) wyników procedur wewnętrznych.
- 41 Właściciel programu posiada procedury lub odesłania do właściwego ustawodawstwa krajowego, które określa mechanizm skutecznego wnoszenia i rozpatrywania skarg i odwołań w związku z wdrażaniem programu certyfikacji lub wydanym certyfikatem zgodności. Procedury te obejmują przekazywanie skarżącemu informacji o przebiegu postępowania i podjętej decyzji oraz informowanie skarżącego o prawie do skutecznego środka odwoławczego przed sądem.
- 42 Programy certyfikacji zawierają postanowienia, zgodnie z którymi wszystkie skargi i odwołania nierozstrzygnięte przez CAB-CB są przekazywane Właścicielowi programu do oceny i rozstrzygnięcia.

43 Właściciel programu informuje Grupę Współpracy na rzecz Europejskiej Tożsamości Cyfrowej o zmianach w programie certyfikacji. Notyfikacja ta zawiera odpowiednie informacje umożliwiające Grupie Współpracy wydawanie zaleceń dla Właściciela programu oraz opinii o zaktualizowanym programie certyfikacji.

44 W ramach grupy Właścicieli programów krajowych programów certyfikacji program certyfikacji podlega okresowemu przeglądowi (przeglądowi wzajemnemu) krajowych programów certyfikacji, aby zapewnić spójne stosowanie wymagań krajowych programów certyfikacji, z uwzględnieniem co najmniej następujących aspektów:

— wniosków o wyjaśnienia kierowanych do Właściciela programu, dotyczących wymagań krajowego programu certyfikacji;

— informacji zwrotnych od interesariuszy i innych zainteresowanych stron;

— reagowania Właściciela krajowego programu certyfikacji na wnioski o informacje.

45 *UWAGA: Obecnie przeglądy wzajemne pozostają poza zakresem Systemu Certyfikacji PL Portfela EUDI.*

46 Okresowy przegląd wzajemny jest koordynowany przez Grupę Współpracy na rzecz Europejskiej Tożsamości Cyfrowej.

47 Zastosowanie mają konsekwencje wszelkich niezgodności opisane w CIR (UE) 2024/2981, art. 17.

4.2 Zakres i cele

48 System Certyfikacji PL Portfela EUDI odnosi się do przedmiotu certyfikacji zdefiniowanego w CIR 2024/2981, art. 3 ust. 2 i 3.

49 System certyfikacji obejmuje ogólne podejście do certyfikacji rozwiązania europejskiego portfela tożsamości cyfrowej.

50 Certyfikacja rozwiązania portfela tożsamości cyfrowej składa się z trzech odrębnych programów certyfikacji (zob.

51 Rysunek 3):

— Program Certyfikacji Funkcjonalnej Europejskiego Portfela Tożsamości Cyfrowej (seria -01)

— Program Certyfikacji Cyberbezpieczeństwa Europejskiego Portfela Tożsamości Cyfrowej (seria -02)

— Program Certyfikacji eID (seria -03)

Ramy schematu	G-01. System Certyfikacji PL Portfela EUDI		
	G-02. Słownik		
	G-03. Organizacja i wsparcie dla właściciela krajowego systemu certyfikacji EUDI		
	G-04. Developing and maintaining the risk register for EUDI Wallet implementation and certification		
	G-05. Wymagania akredytacyjne dla jednostek oceniających zgodność (CAB)		
	GP-01. System Certyfikacji PL Portfela EUDI Program certyfikacji funkcjonalnej	GP-02. System Certyfikacji PL Portfela EUDI Program certyfikacji cyberbezpieczeństwa	GP-03. System Certyfikacji PL Portfela EUDI Program certyfikacji eID
Wymagania dla systemu zarządzania			WZ-03-01. Organisational and technical requirements for eID providers
			WZ-03-02. Organisational and technical requirements for PID providers, including the requirements laid down in Article 5c of the eIDAS Regulation
			WZ-03-03. Organisational and technical requirements for EUDI providers, including the requirements laid down in Article 5c of the eIDAS Regulation
Wymagania produktu oraz usług i procesów związanych z PTC	WP-01-01. Decomposition - EUDI Wallet functional requirements	WP-02-01. Decomposition - EUDI Wallet security requirements	WP-03-01. Requirements for PID Registration and PID/EUDI Wallet life cycle
		WP-02-02. FITCEM protection profile for the application - EUDI Wallet instance	WP-03-02. EUDI Wallet Registration Requirements
		WP-02-03. EU CC Protection Profile for WSCA	WP-03-03. Requirements for eID system (including authentication)
Wymagania dla metod i technik ewaluacji	WM-01-01. Metodyka testowania funkcjonalności Portfela EUDI	WM-02-01. Rozszerzenie metodyki FITCEM na rozwiązanie Portfela EUDI	WM-03-01. Ramy audytu cyberbezpieczeństwa dla dostawców PID
		WM-02-02. Adaptacja oceny opartej na ISO/IEC CEM dla komponentu WSCA	WM-03-02. Ramy audytu cyberbezpieczeństwa dla dostawców eID
			WM-03-03. Ramy audytu cyberbezpieczeństwa dla dostawców Portfela EUDI

Rysunek 3 Ustrukturyzowany widok systemu certyfikacji PL Portfela EUDI

- 52 Niniejszy dokument zawiera szczegółową analizę tego, w jaki sposób ta struktura i jej elementy są zagnieżdżone oraz jak spełniają szczegółowe wymagania właściwych norm i regulacji, aby osiągnąć certyfikację najwyższego poziomu europejskiego portfela tożsamości cyfrowej.
- 53 Każdy program certyfikacji składa się z niezbędnych odniesień do norm (międzynarodowych lub europejskich) lub specyfikacji technicznych, które stanowią zbiór wyspecyfikowanych wymagań dla programu¹.
- 54 Każdy program opiera się na typie programu certyfikacji produktów² według ISO/IEC 17067. Typy przypisane programom certyfikacji Portfela EUDI są następujące (zgodnie z definicją w PN-EN ISO/IEC 17067 – zob. Załącznik A niniejszego dokumentu):
- Program Certyfikacji Funkcjonalnej Europejskiego Portfela Tożsamości Cyfrowej (typ 5);
 - Program Certyfikacji Cyberbezpieczeństwa Europejskiego Portfela Tożsamości Cyfrowej (typ 5);
 - Program Certyfikacji eID (typ 6).
- 55 Program Certyfikacji Funkcjonalnej Europejskiego Portfela Tożsamości Cyfrowej (seria GP-01) to zbiór wymagań i niezbędnych informacji umożliwiających przeprowadzenie oceny zgodności komponentów programowych/sprzętowych jednostki Portfela EUDI. Ustanawia on jeden certyfikat/deklarację zgodności (zob. Rysunek 2) dla dostawców portfeli, jako część całego procesu certyfikacji europejskich portfeli tożsamości cyfrowej.
- 56 Program Certyfikacji Cyberbezpieczeństwa Europejskiego Portfela Tożsamości Cyfrowej (seria GP-02) dostarcza wymagania i niezbędne informacje umożliwiające przeprowadzenie oceny zgodności docelowego produktu. Ustanawia on kolejne stwierdzenie zgodności dla dostawców portfeli, jako część całego procesu certyfikacji europejskich portfeli tożsamości cyfrowej.
- 57 Program Certyfikacji eID (seria GP-03) jest programem nadrzędnym, dostarczającym wytyczne i niezbędne informacje umożliwiające

¹ W przypadku braku norm lub specyfikacji technicznych treść odpowiednich dokumentów będzie opierać się na podejściu „najlepszych praktyk” i będzie ustrukturyzowana zgodnie z ISO/IEC 17007.

² PN-EN ISO/IEC 17067 zawiera uwagę: W niniejszej normie międzynarodowej termin „produkt” może być również odczytywany jako „proces” lub „usługa”, z wyjątkiem przypadków, w których odrębne postanowienia dotyczą „procesów” lub „usług”

przeprowadzenie oceny zgodności w odniesieniu do procedur dostawcy portfela EUDI i dostawcy PID oraz stwierdzenia (stwierdzeń) zgodności systemu eID – zob. Rysunek 2). Program ten będzie ponownie wykorzystywał część wyników uzyskanych w rezultacie działań certyfikacyjnych produktu w ramach programu certyfikacji cyberbezpieczeństwa i funkcjonalnej (serie GP-01 i GP-02). Informacja o stwierdzeniu zgodności rozwiązania portfela EUDI (certyfikat najwyższego poziomu) z wymaganiami zostanie przekazane Komisji Europejskiej i EDICG zgodnie z art. 5d ust. 1 rozporządzenia UE 910/2014.

58 Struktura programu (zob.

59 Rysunek 3) podzielona jest na dwie główne części:

- (a) Sekcja G zawiera wszystkie elementy wspólne dla trzech programów, tj. zasady, procedury i zarządzanie programem, oraz definicję trzech podrzędnych programów certyfikacji (GP-01, GP-02 i GP-03).
- (b) Sekcje WZ, WP i WM są właściwe dla każdego programu i definiują odpowiednie zbiory wymagań w trzech planach, odpowiednio:
 - o dla systemów zarządzania, w stosownych przypadkach;
 - o dla produktów, usług lub procesów;
 - o dla metod i technik oceny.

4.3 Elementy programu według PN-EN ISO/IEC 17067

60 Niniejsza sekcja opiera się na postanowieniach rozporządzenia wykonawczego Komisji (UE) 2024/2981, art. 4 ust. 3 lit. a) i przedstawia szczegółową analizę zgodności z wymaganiami dla programu certyfikacji oraz trzech programów certyfikacji produktów, określonymi w normie, sekcja 6.5. Wszystkie odniesienia użyte w tej sekcji przedstawiono na rysunku (

61 Rysunek 3).

a) **Zakres programu:** Zarówno nadrzędny system certyfikacji opisany w G-01 (niniejszy dokument), jak i każdy program (**GP-01, GP-02, GP-03**) jasno definiują swój zakres: odpowiednio zgodność funkcjonalną, zgodność rozwiązania portfela w zakresie cyberbezpieczeństwa oraz certyfikację systemu eID.

b) **Wymagania dotyczące oceny:** Są one szczegółowo wyspecyfikowane w programach, w planie wymagań dla produktów lub usług. Przykładowo,

plan wymagań cyberbezpieczeństwa produktu składa się z następujących dokumentów:

- (a) WP-02-01. Dekompozycja – wymagania bezpieczeństwa EUDI
- (b) WP-02-02. Profil ochrony FITCEM dla aplikacji – instancja Portfela EUDI
- (c) WP-02-03. Profil ochrony EUCC dla WSCA

- c)** **Wybór działań:** Zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2981, art. 9 ust. 1, certyfikacja jest przeprowadzana zgodnie z PN-EN ISO/IEC 17065. Działania oceny są dalej podzielone w metodyce oceny według technik takich jak audyt, inspekcja, demonstracja i badanie – zob. Załącznik A. Zastosowanie działań oceny we właściwych programach certyfikacji przedstawia Tabela 1.

Tabela 1. Wymagania akredytacyjne w systemie certyfikacji PL Portfela EUDI

	GP-01	GP-02	GP-03
Główne działania oceny	Badania	Badania	Audyt
Norma akredytacyjna dla CAB-CB	PN-ISO/IEC 17065	PN-ISO/IEC 17065 uzupełniona o program EUCC, w stosownych przypadkach	PN-ISO/IEC 17065 uzupełniona o ETSI EN 319 403-1 V2.3.1
Norma akredytacyjna dla CAB-ITSEF	PN-ISO/IEC 17025	PN-ISO/IEC 17025 uzupełniona o program EUCC, w stosownych przypadkach	nie dotyczy

- d)** **Inne wymagania dotyczące klientów:** Wymagania organizacyjne dla klientów (np. dostawców portfela EUDI) są wyspecyfikowane w serii WZ.
- e)** **Wymagania dotyczące jednostek certyfikujących:** system zawiera wymagania dla CAB ³ zdefiniowane we właściwych normach zharmonizowanych (zob. Tabela 1) oraz w G-05.
- f)** **Akredytacja CAB:** niniejszy dokument oraz dodatkowo **G-05** określają wymagania akredytacyjne dla CAB.
- g)** **Metody i procedury:** Wszystkie właściwe metody i procedury oceny są wyspecyfikowane w planach metod i technik oceny. Przykładowo, metody

³ W EUCC rozróżnia się dwa rodzaje CAB: CAB-CB (jednostki certyfikujące) oraz CAB-ITSEF (laboratoria badawcze)

i techniki związane z cyberbezpieczeństwem zawarte są w następujących dokumentach:

- (a) WM-03-01. Ramy audytu cyberbezpieczeństwa dla dostawców Portfela EUDI
- (b) WM-03-02. Ramy audytu cyberbezpieczeństwa dla rejestracji i zarządzania cyklem życia Portfela EUDI
- (c) WM-02-01. Rozszerzenie metodyki FITCEM na rozwiązanie Portfela EUDI wraz z planem badań zgodności;
- (d) WM-02-02. Adaptacja ISO/IEC 15408-4 dla WSCA

- h) **Informacje od wnioskodawców:** CIR (UE) 2024/2981. Wszystkie dokumenty programów certyfikacji (GP-01, -02 i -03) zawierają wykazy dokumentacji wymaganej od wnioskodawców; ponadto, dla programu certyfikacji GP-03 wszystkie właściwe dokumenty serii WZ-03-0x i WP-03-0x określają dokumentację, którą wnioskodawca jest zobowiązany dostarczyć jako dowody uzasadnienia zaufania.
- i) **Treść deklaracji zgodności⁴:** Treść certyfikatu zgodności dla certyfikatu najwyższego poziomu zawarta jest w załączniku VII do CIR (UE) 2024/2981. Szczegółowa treść dla każdego programu certyfikacji zawarta jest w G-01, rozdział 7.
- j) **Warunki, na jakich klient może posługiwać się stwierdzeniem zgodności lub znakami zgodności** – są zdefiniowane w dokumencie G-03 oraz we właściwych sekcjach GP-01, GP-02 i GP-03 w odniesieniu do certyfikowanych obiektów.
- k) **Własność znaków:** Procedury i organizacja techniczna ładu Właściciela systemu/programu zdefiniowane w G-03 ustanawiają zasady posługiwania się certyfikatami zgodności i odpowiednimi znakami używanymi w systemie certyfikacji PL Portfela EUDI. Zasady posługiwania się unijnym znakiem zaufania na certyfikowanym rozwiązaniu Portfela EUDI są określone we właściwych regulacjach UE
- l) **Niezbędne zasoby:** Wymagania kompetencyjne dla personelu CAB oraz niezbędne zasoby do ocen i certyfikacji są zdefiniowane w G-05.

⁴ Wszystkie terminy odnoszące się do stwierdzenia zgodności, tj. deklaracja zgodności, certyfikat, certyfikat zgodności, są synonimami w kontekście programu certyfikacji Portfela EUDI.

- m) **Powiadamianie o wynikach:** G-01 (niniejszy dokument); ponadto procedury powiadamiania Właściciela programu o wynikach oceny i nadzoru są wyspecyfikowane w G-03.
- n) **Postępowanie z niezgodnościami:** G-01 (niniejszy dokument) ustanawia zasady ogólne; dokument zarządzania cyklem życia (WP-03-01), ramy audytu właściwe dla programu certyfikacji GP-03 oraz wszystkie pozostałe programy certyfikacji określają procesy postępowania z niezgodnościami.
- o) **Procedury nadzoru:** Działania nadzorcze są zdefiniowane w CIR (UE) 2024/2981, art. 16. GP-01, GP-02 i GP-03 zawierają postanowienia dotyczące procedur nadzoru.
- p) **Kryteria dostępu:** Zakres dokumentów każdego programu certyfikacji (GP-01, GP-02 i GP-03) oraz wymagania akredytacyjne (G-05) definiują kryteria (tj. uprawnione CAB i interesariuszy) dostępu do programu.
- q) **Publikacja certyfikowanych produktów:** Załącznik V do CIR (UE) 2024/2981 zawiera treść publicznie dostępnych informacji niezbędnych do publikowania repozytorium certyfikowanych produktów. Dodatkowo Właściciel programu publikuje wszystkie certyfikaty/deklaracje zgodności wydane w ramach Systemu Certyfikacji PL Portfela EUDI.
- r) **Umowy:** Odpowiednie dokumenty programów certyfikacji (tj. GP-01, -02 i -03) definiują potrzebę zawierania prawnie wiążących umów między CAB a wnioskodawcami.
- s) **Warunki cyklu życia certyfikacji:** G-01 (niniejszy dokument) definiuje warunki udzielania, utrzymywania, odnawiania, zawieszania lub cofania certyfikatów, doprecyzowane w odpowiednich dokumentach programów (tj. GP-01, -02, -03).
- t) **Rozpatrywanie skarg:** Zagadnienie to jest objęte postanowieniami CIR (UE) 2024/2981, art. 17 oraz G-01 (niniejszy dokument – zob. pkt 42).
- u) **Powoływanie się na certyfikowany produkt** – G-01 (niniejszy dokument) i G-03 zawierają zasady, w jaki sposób klienci mogą powoływać się na certyfikację.
- v) **Przechowywanie zapisów przez Właściciela programu i jednostkę certyfikującą:** G-01 (niniejszy dokument) oraz odpowiednie dokumenty programów (tj. GP-01, -02 i -03) określają wymagania dotyczące przechowywania zapisów.

5 Zarządzanie cyklem życia programu

62 *UWAGA 1: Niniejszy rozdział ustanawia zasady ogólne dla certyfikacji*
rozwiązania Portfela EUDI (certyfikat najwyższego poziomu, zob. Rysunek
1).

63 *UWAGA 2: Wszystkie postanowienia odnoszą się do ról Właściciela programu*
i Właściciela systemu.

5.1 Warunki uczestnictwa CAB w programie certyfikacji

64 CAB jest zobowiązana pomyślnie przejść proces akredytacji w zakresie
właściwego programu certyfikacji. CAB informuje Właściciela programu o
zmianach swojego statusu akredytacji bez zbędnej zwłoki.

65 W należycie uzasadnionych przypadkach CAB może rozpocząć świadczenie
usług oceny lub certyfikacji zgodnie z zasadami określonymi w G-05, sekcja
7.4.

66 Właściciel programu polega na procesie akredytacji NAB, w tym na
nadzorze nad akredytowanymi CAB.

67 Właściciel programu nie przeprowadza żadnej oceny CAB.

68 NAB informuje Właściciela programu o wszelkich zmianach statusu
akredytacji CAB bez zbędnej zwłoki.

5.2 Ogólne zasady dotyczące procesu certyfikacji

69 Certyfikacja rozwiązania Portfela EUDI (certyfikacja najwyższego
poziomu) jest przeprowadzana w ramach programu certyfikacji GP-03.
Wszystkie właściwe certyfikaty lub deklaracje zgodności z programów
certyfikacji GP-01, GP-03, GP-03 i EUCC są wydawane odpowiednio.

70 Podczas składania wniosku o certyfikat najwyższego poziomu Dostawca
Portfela jest zobowiązany do przedłożenia wszystkich odpowiednich i
ważnych certyfikatów lub deklaracji potwierdzających, że w ramach
właściwych programów certyfikacji prowadzone są odpowiednie procesy
oceny i certyfikacji. CAB-CB ocenia zakres oraz ważność tych certyfikatów
lub deklaracji i podejmuje decyzję o przyjęciu wniosku.

71 Zależności pomiędzy statusami certyfikatów wydanych w systemie
certyfikacji Portfela EUDI są określone w odpowiednich sekcjach opisów
poszczególnych programów certyfikacji (tj. GP-01, GP-02 i GP-03).

72 Dopuszcza się przeprowadzenie certyfikacji w odniesieniu do częściowej funkcjonalności rozwiązania Portfela EUDI, a nie kompleksowo dla wszystkich funkcjonalności objętych programami certyfikacji. W takim przypadku każdy dokument certyfikacyjny jednoznacznie wskazuje część funkcjonalności podlegającą certyfikacji.

5.3 Dowody uzasadnienia zaufania ze źródeł zewnętrznych

73 CAB może polegać na zewnętrznych dowodach uzasadnienia zaufania we wszystkich programach certyfikacji oraz w odniesieniu do certyfikatu najwyższego poziomu. Status przypadków uzasadnienia zaufania jest uznawany za wynik uzasadnienia zaufania:

- I. **Pełne poleganie.** Dowody uzasadnienia zaufania dostarczają wystarczających dowodów, że wymaganie jest spełnione. Dla takiego wymagania nie są potrzebne żadne uzupełniające działania ewaluacyjne. CAB-CB dokumentuje podstawy tego ustalenia.
- II. **Częściowe poleganie.** Dowody uzasadnienia zaufania obejmują część wymagania lub zapewniają poziom uzasadnienia zaufania wymagający uzupełnienia. CAB-CB określa i przeprowadza niezbędne uzupełniające działania oceny w ramach oceny.
- III. **Brak polegania.** Dowody uzasadnienia zaufania są niedostępne, nieadekwatne lub nie obejmują wymagania. CAB-CB przeprowadza własną, pełną ocenę wymagania.

74 CAB-CB dokumentuje swoją ocenę i ustalenie stopnia polegania dla każdego dowodu uzasadnienia zaufania w ramach zapisów z oceny. CAB-CB pozostaje w pełni odpowiedzialna za decyzję certyfikacyjną niezależnie od zakresu, w jakim polega na zewnętrznych dowodach uzasadnienia zaufania.

75 Akceptacja dowodów uzasadnienia zaufania w procesie oceny nie może być sprzeczna z wymaganiem PN-EN ISO/IEC 17065, 7.4.5, dotyczącym wyników oceny odnoszących się do certyfikacji zakończonej przed złożeniem wniosku o certyfikację.

5.4 Nadzór

76 Certyfikat najwyższego poziomu podlega corocznym działaniom nadzorczym prowadzonym przez CAB-CB zgodnie z zasadami określonymi w programie certyfikacji GP-03, z uwzględnieniem wyników działań nadzorczych określonych w programach certyfikacji GP-01 i GP-02.

77 Działania nadzorcze istotne dla przedmiotu certyfikacji są określone w odpowiednich programach certyfikacji.

5.5 Obowiązki posiadaczy certyfikatów po certyfikacji

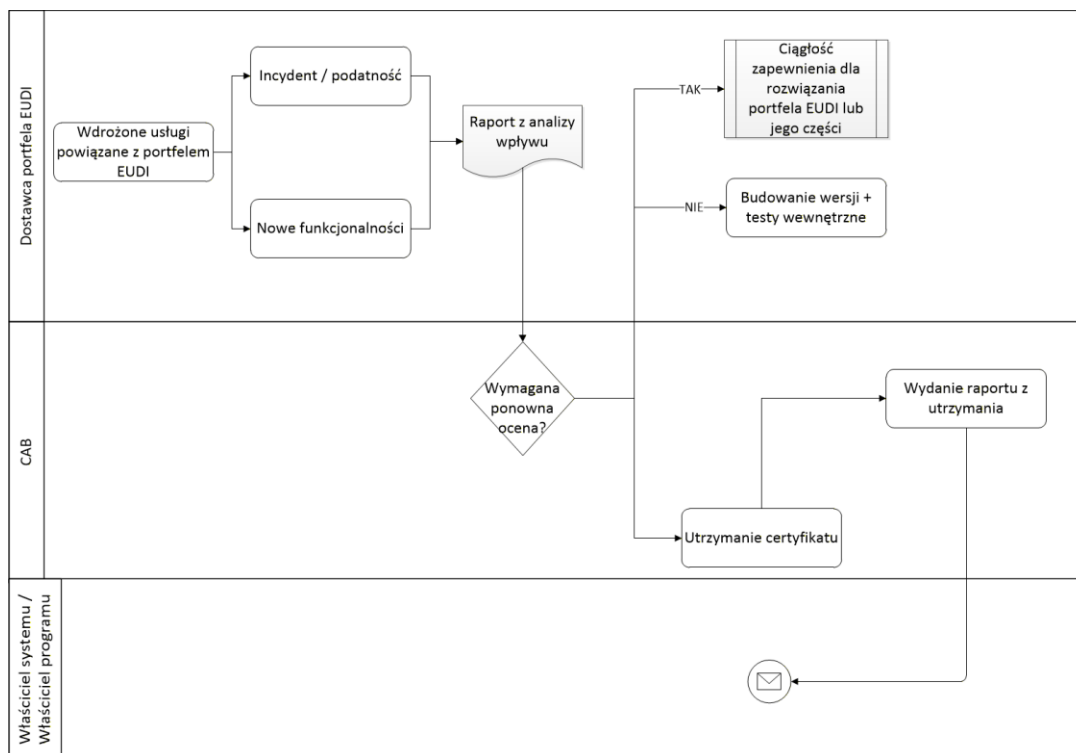
78 Posiadacz certyfikatu:

- o przestrzega właściwych europejskich i krajowych przepisów dotyczących rozwiązania Portfela EUDI, w tym między innymi CIR 2024/2981;
- o ustanawia, wdraża i utrzymuje kanały komunikacji z CAB-CB, CAB-ITSEF (w stosownych przypadkach) oraz Właścicielem programu/systemu w celu wypełniania swoich obowiązków notyfikacyjnych;
- o zapewnia, że istotne informacje dotyczące bezpiecznego użytkowania, certyfikacji i aktualizacji rozwiązania Portfela EUDI, w odniesieniu do certyfikowanej usługi lub certyfikowanej części produktu, są dostępne dla użytkowników końcowych w przystępnym i zrozumiałym języku oraz prezentowane w formacie odpowiednim do ich funkcji;
- o ustanawia, wdraża i utrzymuje ciągły proces identyfikacji, analizy i oceny podatności, które mogą wpływać na rozwiązanie Portfela EUDI, w odniesieniu do certyfikowanej usługi lub certyfikowanej części produktu lub innych produktów lub usług wspierających rozwiązanie Portfela EUDI;
- o ustanawia, wdraża i utrzymuje procedury obsługi podatności oraz współpracuje z CAB-CB i Właścicielem programu w przypadku zidentyfikowania podatności w odniesieniu do certyfikowanej usługi lub certyfikowanej części produktu, lub innych produktów lub usług wspierających rozwiązanie Portfela EUDI;
- o publikuje lub odsyła do publicznie znanych podatności, które mogą wpływać na rozwiązanie Portfela EUDI i dotyczą certyfikowanej usługi lub certyfikowanej części produktu, lub innych produktów lub usług wspierających rozwiązanie Portfela EUDI;
- o zapewnia, aby publikowane lub przywoływane informacje:
 - jasno identyfikowały podatność,

- wskazywały wersje produktu, których podatność dotyczy, lub jego części, lub innego produktu lub usługi wspierającej rozwiązanie Portfela EUDI,
 - zawierały opis środków łagodzących lub aktualizacji dostępnych dla właściwych interesariuszy,
 - nie zawierały żadnych szczegółów umożliwiających bezpośrednie lub pośrednie wykorzystanie podatności.
- o posługuje się znakiem zgodności w odniesieniu do rozwiązania Portfela EUDI, certyfikowanej usługi lub produktu zawierającego certyfikowane części, zgodnie z zasadami określonymi w G-03.

5.6 Zmiany przedmiotu certyfikacji najwyższego poziomu

- 79 Zmiany mające wpływ na rozwiązanie Portfela EUDI, a tym samym na certyfikat najwyższego poziomu, są obsługiwane w ramach regularnego procesu zarządzania zmianami CAB-CB, który stanowi część procesu utrzymania certyfikatu (zob. Rysunek 4).
- 80 W przypadku gdy proces jest inicjowany przez posiadacza certyfikatu, CAB-CB jest odpowiednio powiadamiana i otrzymuje opis zmian w formie raportu analizy wpływu (Impact Analysis Report, IAR).
- 81 Procesy obsługi IAR przez CAB-CB opisane są w odpowiednich programach certyfikacji.



Rysunek 4 Proces zarządzania zmianami wdrożony w systemie certyfikacji

82 Zgodnie z przebiegiem przedstawionym na Rysunku 4, każda zmiana
 83 wynikająca z incydentu bezpieczeństwa lub podatności jest obsługiwana
 przez CAB-CB z poszanowaniem zasady ciągłości uzasadnienia zaufania.

83 *UWAGA: G-03 zawiera opis obsługi podatności technicznych z perspektywy
 Właściciela programu.*

5.7 Postępowanie z niezgodnościami

84 Każde niespełnienie wyspecyfikowanego wymagania przez przedmiot
 certyfikacji jest uznawane za niezgodność.

85 *UWAGA 1: W programach certyfikacji GP-01 i GP-02 ustalenie jest uznawane
 za niezgodność i obsługiwane zgodnie z procedurą postępowania z
 ustaleniami istotnymi.*

86 *UWAGA 2: W kontekście programu certyfikacji GP-03 rozróżnia się
 niezgodności duże i małe.*

87 *UWAGA 3: Ze względu na odmienną charakterystykę niezgodności w
 programach certyfikacji, szczegółowe postanowienia zawarto odpowiednio
 w GP-01, GP-02 i GP-03.*

- 88 CAB-CB zapewnia, aby wszelkie niezgodności zidentyfikowane w odniesieniu do obowiązków posiadacza certyfikatu były obsługiwane zgodnie z postanowieniami umowy oraz PL-EN ISO/IEC 17065.
- 89 W przypadku gdy CAB-CB stwierdzi, że posiadacz certyfikatu nie wypełnia obowiązków nałożonych na podmiot przez właściwe przepisy europejskie lub krajowe albo postanowienia umowne, CAB-CB:
- o formalnie powiadamia posiadacza certyfikatu o istnieniu niezgodności, opisując:
 - konkretny obowiązek – podejrzewany lub udowodniony – którego naruszenie dotyczy,
 - dostępne dowody,
 - możliwy wpływ na zaufanie lub utrzymanie certyfikacji.
 - o żąda od posiadacza certyfikatu dalszych wyjaśnień w sprawie,
 - o w przypadku gdy wyjaśnienia posiadacza certyfikatu nie są wystarczające, ustala maksymalny termin, który nie może przekroczyć trzydziestu (30) dni kalendarzowych, w którym posiadacz certyfikatu:
 - zaproponuje odpowiednie środki naprawcze, oraz
 - zobowiąże się do ich wykonania w rozsądnym czasie.
- 90 W przypadku niedotrzymania terminu, niezadowolających propozycji lub braku odpowiedzi CAB-CB wszczyna procedurę zawieszenia certyfikatu zgodnie z sekcją 5.8.

5.8 Zawieszenie, zakończenie, cofnięcie lub wygaśnięcie certyfikatów

- 91 Certyfikat najwyższego poziomu może zostać zawieszony lub cofnięty w wyniku stwierdzenia niezgodności w certyfikowanym obiekcie lub jego części.
- 92 W przypadku cofnięcia lub zakończenia certyfikatu najwyższego poziomu na wniosek posiadacza certyfikatu, takie działanie jest ostateczne, a certyfikat nie może być przywrócony. Cofnięcie lub zakończenie certyfikatu najwyższego poziomu nie unieważnia automatycznie certyfikatów wydanych dla poszczególnych przedmiotów certyfikacji, pod

warunkiem, że te przedmioty certyfikacji pozostają zgodne z mającymi zastosowanie wymaganiami.

93 W przypadku zawieszenia certyfikatu najwyższego poziomu certyfikat może zostać przywrócony w następstwie formalnego procesu certyfikacji. Proces taki wykazuje, że przyczyny prowadzące do zawieszenia zostały odpowiednio usunięte i rozwiązane oraz że zapewniona jest dalsza zgodność z wymaganiami certyfikacyjnymi.

94 CAB-CB informuje posiadacza certyfikatu i Właściciela systemu o dacie wygaśnięcia certyfikatu najwyższego poziomu oraz bez zbędnej zwłoki podejmuje odpowiednie działania w kierunku ponownej certyfikacji.

95 *UWAGA 1: Wygaśnięcie certyfikatu najwyższego poziomu nie ma żadnego wpływu na ważność innych certyfikatów wydanych w ramach Systemu Certyfikacji PL Portfela EUDI.*

96 *UWAGA 2: Warunki i procedury zawieszenia, cofnięcia/zakończenia lub wygaśnięcia certyfikatów innych niż certyfikat najwyższego poziomu zawarte są w dokumentach dedykowanych programom certyfikacji.*

97 *UWAGA 3: CAB-CB stosuje się do wymagań ISO/IEC 17065 7.11.3 w celu zapewnienia zerwania powiązania między danym produktem lub usługą a certyfikacją.*

5.9 Skargi i odwołania

98 Od każdej decyzji certyfikacyjnej, w tym decyzji dotyczących zawieszenia lub cofnięcia certyfikatu, właściwy interesariusz może się odwołać. Odwołania muszą być należycie uzasadnione poprzez odniesienie do mających zastosowanie wymagań prawnych, wymagań programu lub wymagań systemu, które rzekomo nie zostały spełnione.

99 Odwołanie jest rozpatrywane przez właściwą CAB-CB zgodnie z publicznie dostępnymi procedurami CAB-CB.

100 Właściciel programu nie może zmienić decyzji CAB.

101 Każdy interesariusz ekosystemu Portfela EUDI może złożyć skargę do Właściciela programu dotyczącą dowolnego aspektu Systemu Certyfikacji PL EUDI.

102 Skarga może być rozpatrywana w rozumieniu przepisów postępowania administracyjnego o skargach i wnioskach.

103 *UWAGA 1: G-03 zawiera opis przypadków skarg lub odwołań rozpatrywanych przez Właściciela programu.*

104 *UWAGA 2: Odpowiednie dokumenty programów zawierają opis przypadków odwołań rozpatrywanych przez CAB-CB.*

5.10 Przechowywanie zapisów

105 Okres ważności certyfikatu najwyższego poziomu wynosi trzy lata, zgodnie z postanowieniami GP-03.

106 Okres przechowywania zapisów powstałych w trakcie procesu certyfikacji jest określany zgodnie z właściwymi wymaganiami prawnymi. W przypadku podmiotów publicznych, wszystkie zapisy są przechowywane zgodnie z polską ustawą o narodowym zasobie archiwalnym i archiwach oraz regulacjami wewnętrznymi podmiotu. Podmioty niepubliczne wdrażają regulacje wewnętrzne dotyczące okresu przechowywania zgodne z tą ustawą.

107 *UWAGA 1: Zaleca się określenie okresu przechowywania wszystkich istotnych zapisów tworzonych dla każdej sprawy certyfikacyjnej nie mniej niż pięć lat po zakończeniu procesu certyfikacji.*

108 *UWAGA 2: Dossier certyfikacyjne obejmuje wszystkie istotne działania CAB-CB dotyczące wniosku lub certyfikowanego produktu.*

5.11 Okresowy przegląd programu certyfikacji

109 Właściciel programu przeprowadza okresowe przeglądy systemu certyfikacji Portfela EUDI oraz programów certyfikacji funkcjonujących w ramach systemu.

110 *UWAGA: Procedury przeglądów okresowych dla Właściciela programu są określone w dokumencie G-03.*

5.12 Utrzymanie programu

111 W przypadku gdy proces przeglądu (wewnętrznego lub w formie przeglądu wzajemnego) wykaze niezgodności w programie lub gdy działanie systemu nie spełnia zdefiniowanych kryteriów, Właściciel programu inicjuje proces utrzymania programu, który może skutkować zmianami w samym systemie lub programie, w tym w ich dokumentacji.

112 *UWAGA: Proces utrzymania programu opisany jest w G-03.*

113 Gdy program certyfikacji wprowadza nowe lub zmienione wymagania, Właściciel programu zapewnia dostępność tych informacji dla wszystkich właściwych interesariuszy, w tym CAB.

114 Na podstawie informacji od Właściciela programu CAB-CB zapewnia, aby zmiany dotyczące klienta zostały zakomunikowane wszystkim klientom. CAB-CB weryfikuje wdrożenie zmian przez swoich klientów, w stosownych przypadkach, oraz podejmuje działania wprowadzone przez program w związku ze zmianami.

115 *UWAGA 2: Możliwe działania w związku ze zmianami wpływającymi na certyfikację przedstawiono w PN-EN ISO/IEC 17065, 10.1.3.*

5.13 Przegląd wzajemny

116 *Opis (ewentualnego) procesu przeglądu wzajemnego zawarty jest w G-03.*

6 Przegląd metod oceny zgodności, specyfikacji i raportowania

6.1 Postanowienia ogólne

117 Niniejszy rozdział zawiera ujednolicony przegląd zestawu narzędzi oceny zgodności wspierającego program certyfikacji Portfela EUDI. Ustanawia metody, wymagania kompetencyjne, kryteria decyzyjne oraz zasady raportowania, które stanowią podstawę wszystkich działań w ramach programów: funkcjonalnego, cyberbezpieczeństwa i eID.

118 Ogólny opis mających zastosowanie metod oceny zgodności zawarty jest w Załączniku A.

6.2 Elementy wymagane do zdefiniowania w ramach metod oceny zgodności

119 Aby zapewnić zharmonizowane wdrożenie, każda metoda stosowana w ramach programu jednoznacznie definiuje następujące elementy:

- (a) Wymagania kompetencyjne: Kompetencje są definiowane dla wszystkich osób zaangażowanych w ocenę, na podstawie metody mającej zastosowanie do właściwego programu certyfikacji.
- (b) Warunki outsourcingu: Co do zasady outsourcing nie jest dozwolony, chyba że jest wyraźnie dopuszczony w ramach normatywnych metody. Tam, gdzie jest dozwolony, mające zastosowanie wymagania są opisane we właściwym programie certyfikacji.
- (c) Kryteria zaliczenia/niezaliczenia: Dla każdego działania oceny metoda definiuje mające zastosowanie kryteria zaliczenia/niezaliczenia oraz opisuje ich wpływ na ważność certyfikatu.

6.3 Obowiązkowe elementy raportów

120 Obowiązkowe elementy raportowania są definiowane zgodnie z metodą oceny zgodności. Program certyfikacji może dodać inne stosowne wymagania, w stosownych przypadkach.

121 Raporty z badań zawierają następujące elementy obowiązkowe (zob. ISO/IEC 17025):

- o tytuł: raport z badań / raport z pobierania próbek;
- o nazwa i adres laboratorium badawczego;
- o miejsce wykonywania działalności laboratoryjnej;

- o niepowtarzalna identyfikacja zapewniająca, że wszystkie elementy raportu są rozpoznawane jako część kompletnego raportu, oraz wyraźne oznaczenie końca raportu;
- o nazwa i dane kontaktowe klienta;
- o identyfikacja metody;
- o daty wykonania działalności laboratoryjnej;
- o data wydania raportu;
- o oświadczenie, że wyniki odnoszą się wyłącznie do badanych lub pobranych obiektów;
- o wyniki wraz z, w stosownych przypadkach, jednostkami miar;
- o identyfikacja osoby (osób) autoryzującej raport;
- o wyraźne oznaczenie, gdy wyniki badań pochodzą od dostawców zewnętrznych, w tym od klientów.

122 Raport z audytu systemu zarządzania zawiera następujące elementy obowiązkowe (zob. ISO/IEC 17021-1):

- o identyfikacja jednostki certyfikującej;
- o nazwa i adres klienta oraz przedstawiciela kierownictwa klienta;
- o rodzaj audytu (np. audyt początkowy, nadzorczy lub ponownej certyfikacji);
- o kryteria audytu;
- o cele audytu;
- o zakres audytu, w szczególności identyfikacja audytowanych jednostek organizacyjnych lub funkcjonalnych lub procesów oraz czas trwania audytu;
- o identyfikacja audytora wiodącego, członków zespołu audytowego i wszelkich osób towarzyszących;
- o daty i miejsca prowadzenia działań audytowych (na miejscu lub zdalnie);
- o dowody z audytu, ustalenia i wnioski, spójne z wymaganymi elementami audytu;
- o wszelkie nierozstrzygnięte kwestie, jeżeli zostały zidentyfikowane.

123 Dokumentacja certyfikacji dotyczącej produktu, usługi lub procesu przekazywana klientowi zawiera następujące elementy obowiązkowe (zob. ISO/IEC 17065):

- o nazwa i adres jednostki certyfikującej;
- o data udzielenia certyfikacji (data nie może być wcześniejsza niż data zakończenia podejmowania decyzji certyfikacyjnej);
- o nazwa i adres klienta;

- o zakres certyfikacji;
- o termin lub data wygaśnięcia certyfikacji, jeżeli certyfikacja wygasa po ustalonym okresie;

124 Dodatkowo raport certyfikacyjny dla przedmiotu zgodności zawiera szczegółowe informacje wymagane przez programy certyfikacji (zob. GP-01, GP-02, GP-03).

6.4 Szablon oceny zgodności dedykowany programom certyfikacji

125 Aby zapewnić spójne wdrażanie programów certyfikacji, wprowadza się tabelę podstawowych charakterystyk programu.

Zagadnienie	Wymagany opis	Wymagane szczegóły
Przedmiot oceny zgodności	Jednoznaczna identyfikacja ocenianego komponentu	Odniesienie do modelu kompozytowego, w stosownych przypadkach
Metodyka oceny zgodności	Wybór metodyki spośród metodyk opisanych w Załączniku A	Uzasadnienie wyboru tej metodyki
Kryteria bezstronności	Identyfikacja kryteriów bezstronności wyłącznie wówczas, gdy stanowią one uzupełnienie ogólnych kryteriów bezstronności normy oceny zgodności.	
Kryteria poufności	Identyfikacja kryteriów poufności wyłącznie wówczas, gdy stanowią one uzupełnienie ogólnych kryteriów bezstronności normy oceny zgodności.	
Wymagania kompetencyjne	Osoby wykonujące metody oceny zgodności.	Specyfikacja wymagań kompetencyjnych lub odniesienie do właściwych źródeł.
Kryteria zaliczenia/niezaliczenia	Ogólny opis kryteriów zaliczenia/niezaliczenia	Odniesienie do właściwych norm lub dokumentów WM-0x
Cykl życia certyfikatu	Kryteria zawieszenia / cofnięcia / odnowienia, w stosownych przypadkach	Opis warunków we wszystkich właściwych programach certyfikacji

Raportowanie	Elementy raportowania – odniesienie do pkt 6.3 + elementy dodatkowe, gdy są wymagane	Szczegóły dotyczące formatu
Zależności	Zależności od innych przedmiotów oceny zgodności	Opis

7 Analiza zgodności

7.1 Zgodność z rozporządzeniem eIDAS i właściwymi aktami wykonawczymi

7.1.1 Zgodność z aktem wykonawczym (CIR (UE) 2024/2981)

126 Program certyfikacji został zaprojektowany tak, aby był w pełni zgodny ze specyfikacjami i procedurami ustanowionymi rozporządzeniem wykonawczym Komisji (UE) 2024/2981 w sprawie certyfikacji europejskich portfeli tożsamości cyfrowej. Poniższa analiza szczegółowo przedstawia, w jaki sposób wymagania aktu wykonawczego są spełniane przez strukturę programu certyfikacji.

127 **Artykuł 1: Przedmiot i zakres**

128 Wymaganie: Ustala zakres solidnych ram certyfikacji portfeli

129 Zgodność: Cały system certyfikacji, zarządzany przez G-01, został zaprojektowany w celu ustanowienia takich ram. Trzy filary (GP-01, GP-02, GP-03) łącznie obejmują pełny zakres wymagany do certyfikacji rozwiązania portfela EUDI i bazowego systemu eID.

130 **Artykuł 2: Definicje**

131 Wymaganie: Zawiera kluczowe definicje dla rozporządzenia.

132 Zgodność: G-02 (Słownik) jest dokumentem dedykowanym ustanowieniu zbioru terminów istotnych dla programu certyfikacji. G-02 uwzględnia wszystkie definicje z art. 2 CIR (UE) 2024/2981 oraz dodaje odpowiednie terminy i ich definicje, w razie potrzeby.

133 **Artykuł 3: Ustanowienie krajowych programów certyfikacji**

134 Wymaganie 3(1): Państwa członkowskie wyznaczają Właściciela programu.

135 Zgodność: G-01 wyznacza Właściciela programu/Właściciela systemu i określa obowiązki tej roli. Podmiot pełniący tę rolę zostaje wskazany w polskim akcie prawnym.

136 Wymaganie 3(2): Przedmiotem certyfikacji jest dostarczanie i eksploatacja rozwiązań portfela oraz systemów eID.

137 Zgodność: Jest to w pełni objęte trójfilarową strukturą:

(a) Seria GP-01: obejmuje funkcjonalne dostarczanie i eksploatację Portfela EUDI.

(b) Seria GP-02: obejmuje cyberbezpieczeństwo rozwiązania portfela EUDI.

(c) Seria GP-03: obejmuje certyfikację bazowego systemu eID.

138 Wymaganie 3(3): Przedmiot certyfikacji obejmuje określone elementy.

139 Zgodność:

(a) Komponenty programowe: objęte dokumentami WP-01-01 Dekompozycja – wymagania funkcjonalne Portfela EUDI oraz WP-02-01 Dekompozycja – wymagania bezpieczeństwa Portfela EUDI, WP-02-02, -03 (odpowiednie profile ochrony).

(b) Komponenty sprzętowe: objęte profilem ochrony dla WSCD, certyfikowanym zewnętrznie. Dodatkowo odpowiednie założenia dotyczące platform, na których działają komponenty programowe, o których mowa w lit. a), lub na których polegają one przy operacjach krytycznych, omówiono w serii dokumentów WP-02.

(c) Procesy wspierające dostarczanie i eksploatację rozwiązania portfela, wyrażnie przywołane w CIR (UE) 2015/1502: szczegółowo objęte serią GP-03, w szczególności WP-03-01 (Zarządzanie cyklem życia), WP-03-02 (Rejestracja w Portfelu EUDI) oraz WP-03-03 (Zarządzanie środkami eID).

140 **ROZDZIAŁ II KRAJOWE PROGRAMY CERTYFIKACJI**

141 Wymaganie 3(4): Krajowe programy certyfikacji zawierają opis szczególnej architektury rozwiązań portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one dostarczane.

142 Zgodność:

143 Zob. Załącznik A w niniejszym dokumencie.

144 Wymaganie 3(5): [Szczególna architektura rozwiązania portfela] w ramach programu musi definiować określone elementy.

145 Zgodność:

(a) szczególna architektura rozwiązania portfela i systemu identyfikacji elektronicznej: zob. Załącznik A niniejszego dokumentu.

- (b) środki bezpieczeństwa powiązane z poziomami uzasadnienia zaufania określonymi w art. 8 rozporządzenia (UE) nr 910/2014: są zdefiniowane w GP-03 i zmapowane do poziomów uzasadnienia zaufania oznaczonych jako <potwierdzenie tożsamości>.
- (c) 3(6) i 3(7) plan(y) oceny sporządzone zgodnie z sekcją 7.4.1 EN ISO/IEC 17065:2012: będą opracowywane jako działanie wstępne każdej oceny w ramach programów GP-01, GP-02 i GP-03..
- (d) wymagania bezpieczeństwa niezbędne do zaadresowania ryzyk i zagrożeń cyberbezpieczeństwa wymienionych w rejestrze ryzyk określonym w załączniku I: metodyka opracowywania i utrzymywania rejestru ryzyk zawarta jest w G-04; dodatkowo szczegółowe zagrożenia i ryzyka są uwzględniane jako część definicji problemu bezpieczeństwa we właściwych profilach ochrony (seria dokumentów WP-02) oraz dokumentach ram audytu (seria dokumentów GP-03). Dokumentacja, którą dostawca portfela przedkłada jako dowody uzasadnienia zaufania.
- (e) Mapowanie środków bezpieczeństwa: zdefiniowane we właściwych częściach serii dokumentów WP-02 opisujących funkcjonalność bezpieczeństwa rozwiązania Portfela EUDI.
- (f) Uzasadnienie oceny ryzyka: objęte właściwymi częściami serii dokumentów WP-02 omawiającymi poprawność i wystarczalność funkcjonalności bezpieczeństwa.

146 **Artykuł 4: Wymagania ogólne**

147 Wymaganie 4(1) i 4(2): Programy obejmują wymagania funkcjonalne, cyberbezpieczeństwa i ochrony danych z wykorzystaniem europejskich programów certyfikacji cyberbezpieczeństwa, w stosownych przypadkach.

148 Zgodność: Program EUCC zdefiniowany w CIR (UE) 2024/2981 jest wykorzystywany do certyfikacji określonych komponentów jednostki Portfela EUDI; kompozytowy przedmiot oceny (tj. instancja portfela + WSCA + WSCD i odpowiednie interfejsy), funkcjonalność Portfela EUDI oraz system eID będą certyfikowane w ramach dedykowanych krajowych programów certyfikacji. W miarę możliwości programy certyfikacji opierają się na właściwych normach europejskich lub międzynarodowych lub specyfikacjach technicznych (np. EN 17640:2022 +A1:2026 – metodyka oceny cyberbezpieczeństwa w ustalonym czasie dla cyberbezpieczeństwa kompozytowego TOE).

- 149 Wymaganie 4(3)(a): Krajowe programy certyfikacji określają elementy wymienione w sekcji 6.5 PN-EN ISO/IEC 17067:2013;
- 150 Zgodność: zob. sekcja 4.3 G-01 (niniejszy dokument)
- 151 Wymaganie 4(3)(b): Krajowe programy certyfikacji są wdrażane jako program typu 6 (PN-EN ISO/IEC 17067).
- 152 Zgodność: G-01 (niniejszy dokument) wyraźnie stwierdza, że program certyfikacji jest programem typu 6 dla certyfikatu najwyższego poziomu (GP-03), co obejmuje certyfikację początkową i późniejsze działania nadzorcze dotyczące zarówno certyfikowanego produktu, jak i powiązanych usług. Procesy certyfikacji są zdefiniowane w GP-01, GP-02 i GP-03. Ramy nadzoru są zdefiniowane w G-01 (niniejszy dokument).
- 153 Wymagania 4(4)(a), (c), (d): Krajowe programy certyfikacji (definiują) wymagania dla uprawnionych dostawców.
- 154 Zgodność: Zasady ładu organizacyjnego są zdefiniowane w G-01. Wymagania organizacyjne i techniczne dla dostawcy Portfela EUDI opisano w dokumencie WZ-01, natomiast takie wymagania dla dostawców eID, PID i innych usług wspierających mają zostać zdefiniowane w serii dokumentów WP-03.
- 155 Wymaganie 4(4)(b): Krajowe programy certyfikacji zapewniają, aby jako znak zgodności używany był wyłącznie znak zaufania.
- 156 Zgodność: G-03 definiuje odpowiednie charakterystyki znaku krajowego oraz warunki jego używania. Znak zaufania zdefiniowany w rozporządzeniu wykonawczym Komisji 2024/2981 będzie używany wyłącznie dla certyfikatu najwyższego poziomu.
- 157 Wymaganie 4(4)(e): Krajowe programy certyfikacji definiują zakresy odpowiedzialności oraz środki prawne, a także zawierają odesłania do mającego zastosowanie ustawodawstwa krajowego, które definiuje zakresy odpowiedzialności i możliwe działania prawne w przypadku nieuprawnionego posługiwania się certyfikacją w ramach programu.
- 158 Zgodność: podlega dedykowanemu polskiemu aktowi prawnemu ustanawiającemu System Certyfikacji PL Portfela EUDI.
- 159 **Artykuł 5: Zarządzanie incydentami i podatnościami**
- 160 Wymagania 5(2) do (7) oraz (9) dotyczące posiadaczy certyfikatów.

161 Zgodność: Wymagania te są zdefiniowane w dokumentach wymagań organizacyjnych: WZ-01 oraz serii dokumentów WZ-03 dotyczących odpowiednich dostawców. Odpowiadające im ramy audytu (serie dokumentów WM-02 i WM-03) służą do weryfikacji poprawnego wdrożenia przez nich wymagań dotyczących obsługi incydentów i podatności.

162 Wymaganie 5(8) Krajowe programy certyfikacji ustanawiają wymagania dotyczące ujawniania podatności mające zastosowanie do jednostek certyfikujących.

163 Zgodność: Wymaganie to jest zawarte w programie certyfikacji GP-02.

164 **Artykuł 6: Utrzymanie krajowych programów certyfikacji**

165 Wymaganie 6(1)(2): Krajowe programy certyfikacji ustanawiają i wdrażają procesy okresowego przeglądu, utrzymania i zarządzania zmianami.

166 Zgodność: Jest to podstawowa funkcja Właściciela programu i całego modelu ładu organizacyjnego, opisanego w G-01 (niniejszy dokument), a odpowiednie procedury ustanowiono w G-03.

167 **ROZDZIAŁ III – WYMAGANIA DOTYCZĄCE WŁAŚCICIELI PROGRAMÓW**

168 **Artykuł 7: Wymagania ogólne**

169 Wymagania 7(1) do (4): Krajowy program certyfikacji definiuje obowiązki Właściciela programu.

170 Zgodność: Obowiązki te opisano w G-01, sekcja 4.1.

171 **ROZDZIAŁ IV – WYMAGANIA DOTYCZĄCE DOSTAWCÓW**

172 **Artykuł 8: Wymagania ogólne**

173 Wymagania 8(1)(2) oraz (4): Krajowe programy certyfikacji zawierają wymagania cyberbezpieczeństwa oparte na ocenie ryzyka każdej konkretnej wspieranej architektury.

174 Zgodność: Odpowiednie wymagania są objęte serią dokumentów GP-02. Ramy bezpieczeństwa dla rozwiązania eID objęte są GP-03-03 (Wymagania bezpieczeństwa dla środków eID). Są one wspierane przez G-04 (Opracowanie i utrzymanie rejestru ryzyk Portfela EUDI). Odpowiadające im ramy audytu (serie dokumentów WM-02 i WM-03) będą wykorzystywane do weryfikacji poprawnego wdrożenia wymagań bezpieczeństwa w produkcie i powiązanych usługach.

175 Wymaganie 8(3): Krajowe programy certyfikacji ustanawiają kryteria bezpieczeństwa, które obejmują następujące wymagania, tj. obszerną listę wymagań dla dostawców, w tym zarządzanie ryzykiem, polityki dotyczące zmian, obsługę podatności, zarządzanie zasobami ludzkimi, środowisko operacyjne itd.

176 Zgodność: Są one wyspecyfikowane w serii dokumentów WZ zawierających wymagania organizacyjne i techniczne dedykowane dostawcom, tj. WZ-01 (dostawcy Portfela EUDI), WZ-03-01 (dostawcy eID), WZ-03-02 (dostawcy PID) oraz WZ-03-03 (dostawcy usług wspierających system eID). Ich wdrożenie jest weryfikowane za pomocą odpowiednich ram audytu (seria dokumentów WM).

177 Wymaganie 8(5): Krajowe programy certyfikacji wymagają, aby wnioskodawca ubiegający się o certyfikację dostarczył jednostce certyfikującej lub w inny sposób udostępnił następujące informacje i dokumentację (..):

178 Zgodność: struktura formularzy wniosków zawierających odpowiednie informacje opisane w rozporządzeniu wykonawczym Komisji 2024/2981 jest dostarczana przez CAB-CB na podstawie postanowień GP-01, GP-02 i GP-03.

179 **ROZDZIAŁ V – WYMAGANIA DOTYCZĄCE JEDNOSTEK CERTYFIKUJĄCYCH**

180 **Artykuł 9: Wymagania ogólne**

181 Wymagania 9(1), (2) oraz (3): Jednostki certyfikujące są akredytowane przez krajowe jednostki akredytujące zgodnie z EN ISO/IEC 17065:2012, pod warunkiem spełnienia wymagań akredytacyjnych.

182 Zgodność: Ramy akredytacji są zdefiniowane w G-01 (niniejszy dokument). Wszystkie wymagania dotyczące CAB (w tym działania nadzorcze) są skonsolidowane i uszczegółowione w G-05 (Wymagania akredytacyjne dla CAB).

183 Wymagania 10 i 11: dotyczące podwykonawstwa i notyfikacji do organu nadzoru.

184 Zgodność:

- (a) Zasady podwykonawstwa są zdefiniowane we właściwych programach certyfikacji funkcjonujących w ramach systemu certyfikacji PL Portfela EUDI.

(b) Właściciel systemu zostanie wyznaczony w dedykowanym polskim akcie prawnym.

185 Wymaganie 12: dotyczące zarządzania incydentami i podatnościami.

186 Zgodność: Jest zawarte w programie certyfikacji cyberbezpieczeństwa GP-02 i programie certyfikacji eID GP-03; dodatkowo G-03 zawiera informacje o obowiązku Właściciela programu w zakresie polityki skoordynowanego ujawniania podatności w ekosystemie PL Portfela EUDI.

187 **ROZDZIAŁ VI – DZIAŁANIA W ZAKRESIE OCENY ZGODNOŚCI**

188 **Artykuł 13: Działania oceny**

189 Wymagania 13(1) do (4): Krajowe programy certyfikacji zawierają metody i procedury stosowane przez jednostki oceniające zgodność podczas prowadzenia działań oceny (..)

190 Zgodność: Wszystkie metody i procedury oceny są zdefiniowane w programach certyfikacji (GP-01, GP-02 i GP-03). Szczegółowe opisy zawarte są w serii dokumentów WM w każdym programie certyfikacji.

191 **Artykuł 14: Działania certyfikacyjne**

192 Wymaganie 14(1): Krajowe programy certyfikacji ustanawiają działanie atestacyjne na potrzeby wydania certyfikatu zgodności (..)

193 Zgodność: Wymaganie to jest zaadresowane w GP-01, GP-02 i GP-03, które zawierają odpowiednie specyfikacje programów certyfikacji.

194 Wymaganie 14(2): Raport z oceny certyfikacyjnej może zostać udostępniony Grupie Współpracy na rzecz Europejskiej Tożsamości Cyfrowej i Komisji Europejskiej.

195 Zgodność: Wymaganie to jest zaadresowane w GP-03; dotyczy końcowego raportu z oceny zgodności dla certyfikatu najwyższego poziomu.

196 **Artykuł 15: Skargi i odwołania – podlegają prawu krajowemu**

197 **Artykuł 16: Działania nadzorcze**

198 Wymaganie: Działania nadzorcze są realizowane przez jednostki certyfikujące.

199 Zgodność: Ramy ogólne zdefiniowano w G-01, sekcja 4.1. Szczegółowe specyfikacje wdrożono we wszystkich programach certyfikacji (GP-01, GP-

02 i GP-03) oraz odpowiednich dokumentach dotyczących ram audytu (seria WM).

200 **Artykuł 17: Konsekwencje niezgodności**

201 Wymaganie: Krajowe programy certyfikacji określają konsekwencje niezgodności certyfikowanego rozwiązania portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one dostarczane, z wymaganiami określonymi w rozporządzeniu wykonawczym Komisji 2024/2981

202 Zgodność: Odpowiednie konsekwencje przywołano w G-01 (niniejszy dokument), zob. sekcja 5.8.

203 **ROZDZIAŁ VII – CYKL ŻYCIA CERTYFIKACJI**

204 **Artykuł 18: Cykl życia certyfikacji**

205 Wymaganie 18(1): Ważność certyfikatów zgodności wydawanych w ramach krajowych programów certyfikacji podlega regularnym działaniom oceny prowadzonym przez jednostkę certyfikującą (..)

206 Wymaganie 18(2): Krajowe programy certyfikacji zawierają proces ponownej certyfikacji rozwiązań portfela oraz systemu identyfikacji elektronicznej, w ramach którego są one dostarczane, na wniosek posiadacza certyfikatu zgodności przed wygaśnięciem pierwotnego certyfikatu zgodności.

207 Wymaganie 18(3): Krajowe programy certyfikacji zawierają proces zarządzania zmianami w certyfikowanym rozwiązaniu portfela oraz systemie identyfikacji elektronicznej, w ramach którego są one dostarczane.

208 Wymaganie 18(4): Krajowe programy certyfikacji zawierają proces ocen specjalnych zgodnie z PN-EN ISO/IEC 17065. Proces ocen specjalnych obejmuje wybór działań do wykonania w celu zaadresowania konkretnego zagrożenia, które wywołało ocenę specjalną.

209 Wymaganie 18(5): Krajowe programy certyfikacji określają zasady dotyczące anulowania certyfikatu zgodności.

210 Zgodność: Wszystkie procesy wskazane w art. 18 są wyspecyfikowane w programach certyfikacji GP-01, GP-02 i GP-03.

211 **ROZDZIAŁ VIII – PROWADZENIE REJESTRÓW I OCHRONA INFORMACJI**

212 **Artykuł 19: Przechowywanie zapisów**

213 Wymaganie 19(1): Krajowe programy certyfikacji zawierają wymagania dla jednostek certyfikujących dotyczące systemu rejestrowania wszystkich istotnych informacji powstałych w związku z działaniami oceny zgodności.

214 Zgodność: Zasady ogólne zawarto w G-01. Wymagania te są nakładane na CAB w programach certyfikacji GP-01, GP-02 i GP-03.

215 Wymaganie 19(2) oraz (3): Krajowe programy certyfikacji określają wymagania dla posiadacza certyfikatu zgodności dotyczące bezpiecznego przechowywania następujących informacji na potrzeby rozporządzenia wykonawczego Komisji 2024/2981 (..)

216 Zgodność: Odpowiednie obowiązki posiadaczy certyfikatów zawarto w G-01 (niniejszy dokument) oraz w odpowiednich formularzach wniosków definiowanych przez CAB-CB na podstawie postanowień programów certyfikacji (GP-01, GP-02 i GP-03).

217 **Artykuł 20: Ochrona informacji**

218 Wymaganie: (..) wszystkie osoby lub organizacje, którym udzielono dostępu do informacji w ramach wykonywania działań w ramach krajowego programu certyfikacji, są zobowiązane do zapewnienia bezpieczeństwa i ochrony tajemnic handlowych oraz innych informacji poufnych, a także do poszanowania praw własności intelektualnej, oraz do podjęcia niezbędnych i odpowiednich środków technicznych i organizacyjnych w celu zapewnienia tej poufności.

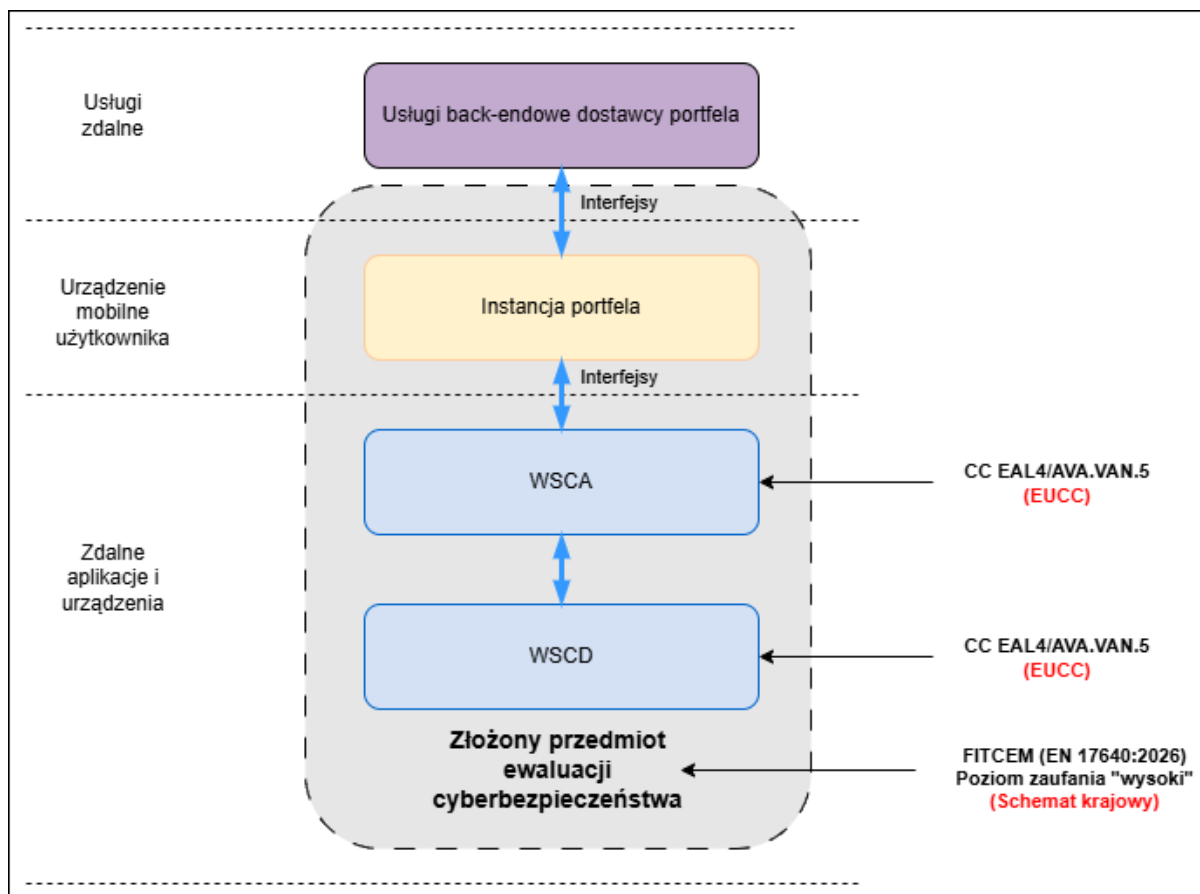
219 Zgodność: Zostanie osiągnięta poprzez odpowiednie procedury wdrożone przez Właściciela programu i CAB, uzupełnione klauzulami poufności zawartymi w umowach między CAB a podmiotem ubiegającym się o certyfikat.

7.2 Zgodność z Aktem o cyberbezpieczeństwie (UE) (art. 54 ust. 1 – Elementy europejskich programów certyfikacji cyberbezpieczeństwa)

220 Program **GP-02 (Program Certyfikacji Cyberbezpieczeństwa Portfela EUDI)** został zaprojektowany tak, aby był zgodny⁵ z art. 54 ust. 1 CSA.

⁵ GP-02 odnosi się do złożonego przedmiotu oceny, w którym są dwa komponenty (WSCD i WSCA) podlegające certyfikacji w programie EUCC, Jednakże GP-02 – jako krajowy program certyfikacji -nie podlega regulacjom unijnym w zakresie certyfikacji cyberbezpieczeństwa; intencją tego podrozdziału jest

- 221 Europejski program certyfikacji cyberbezpieczeństwa zawiera co najmniej następujące elementy:
- 222 **Przedmiot i zakres:** Zakres programu jest zdefiniowany w sekcji wprowadzającej GP-02.
- 223 **b) Cel programu:** Celem jest certyfikacja funkcjonalności cyberbezpieczeństwa komponentów Portfela EUDI.
- 224 **c) Odniesienia do norm:** Dla programu EUCC zastosowanie mają Common Criteria/Common Evaluation Methodology, CC/CEM:2022 wydanie 1 (odpowiednio ISO/IEC 15408:2022/ISO/IEC 18045:2022); dla krajowego programu certyfikacji cyberbezpieczeństwa zastosowanie ma EN 17640:2022 +A1:2026.
- 225 **d) Poziomy uzasadnienia zaufania:** Program wyraźnie celuje w wysoki poziom uzasadnienia zaufania, w szczególności AVA_VAN.5 dla certyfikacji związanych z EUCC, oraz poziom uzasadnienia zaufania „wysoki” zgodnie z definicją zawartą w rozporządzeniu (UE) 2019/881 dla części GP-02 związanej z FITCEM (zob. Rysunek 5).



Rysunek 5 Koncepcja TOE dla GP-02

- 226 **e) Samoocena:** Programy opierają się na ocenie strony trzeciej przez akredytowane CAB; samoocena nie jest dozwolona dla wymaganego poziomu uzasadnienia zaufania.
- 227 **f) Wymagania dotyczące CAB:** Są one uszczegółowione w G-05, zapewniając, aby CAB posiadały kompetencje techniczne do oceny szczegółowych wymagań.
- 228 **g) Kryteria i metody oceny:** Są one wyspecyfikowane w serii dokumentów WM-02.
- 229 **h) Informacje od wnioskodawców:** Są one wyspecyfikowane w GP-02 i odpowiednich formularzach wniosków.
- 230 **i) Znaki lub etykiety:** Model ładu organizacyjnego (G-01) wraz ze szczegółowymi procedurami w G-03 definiuje warunki używania znaku certyfikacji związanego z programem certyfikacji GP-02.
- 231 **j) Zasady monitorowania zgodności** są wyspecyfikowane w programie certyfikacji GP-02.

- 232 **k) Warunki cyklu życia certyfikacji** są wyspecyfikowane w programie certyfikacji GP-02.
- 233 **l) Konsekwencje niezgodności:** Model ładu organizacyjnego zawarty w G-01 ustanawia zasady postępowania z certyfikowanymi produktami, w których stwierdzono niezgodność.
- 234 **m) Zgłaszanie podatności:** Model ładu organizacyjnego zawarty w G-01, a dalej w G-03, ustanawia zasady zgłaszania nowo odkrytych podatności i zarządzania nimi.
- 235 **n) Przechowywanie zapisów:** Model ładu organizacyjnego zawarty w G-01 określa zasady przechowywania zapisów przez CAB. Dodatkowo szczegółowe postanowienia dotyczące przechowywania zapisów znajdują się w każdym programie certyfikacji.
- 236 **o) Identyfikacja innych programów:** Program cyberbezpieczeństwa (GP-02) identyfikuje relację między różnymi podprogramami (opartym na EUCC oraz krajowym programem certyfikacji cyberbezpieczeństwa opartym na EN 17640/AMD1).
- 237 **p) Treść i format certyfikatów:** Zostaną zdefiniowane przez CAB-CB na podstawie postanowień zawartych w GP-02.
- 238 **q) Dostępność dokumentacji:** Wymagania organizacyjne będą nakazywać okres dostępności całej istotnej dokumentacji zgodnie z CIR (UE) 2024/2981, art. 19.
- 239 **r) Maksymalny okres ważności:** Jest zdefiniowany w modelu ładu organizacyjnego zawartym w G-01 (niniejszy dokument) dla certyfikatu najwyższego poziomu oraz w każdym programie certyfikacji dla poszczególnych krajowych certyfikatów/deklaracji zgodności.
- 240 **s) Polityka ujawniania:** Model ładu organizacyjnego zawarty w G-01 definiuje politykę ujawniania statusu certyfikatów (wydany, zmieniony, zawieszony, cofnięty). Dodatkowo każdy program certyfikacji zawiera szczegółowe postanowienia dotyczące warunków cykli życia certyfikatów.
- 241 **t) Wzajemne uznawanie:** Część związana z EUCC – podlega automatycznemu wzajemnemu uznawaniu w całej UE na podstawie przepisów CSA; część dotycząca krajowego programu certyfikacji cyberbezpieczeństwa – podlega dalszym dyskusjom między państwami członkowskimi.

- 242 **u) Mechanizm oceny wzajemnej:** jest ustanowiony jako część modelu ładu organizacyjnego zdefiniowanego w G-01 oraz przepisów CSA dotyczących „oceny wzajemnej” (zastosowano poziom uzasadnienia zaufania „wysoki”).
- 243 **v) Informacje uzupełniające:** GP-02 definiuje procedury przekazywania użytkownikom uzupełniających informacji dotyczących cyberbezpieczeństwa (zob. art. 55 CSA).

Załącznik A Metody i techniki oceny zgodności

A.1. Terminy dotyczące oceny zgodności

UWAGA: Wszystkie definicje pochodzą z EN-ISO/IEC 17000:2020, chyba że wskazano inaczej.

244 **Ocena zgodności** – wykazanie, że **wyspecyfikowane wymagania** zostały spełnione

245 **Przedmiot oceny zgodności** – jednostka, do której **wyspecyfikowane wymagania** mają zastosowanie

246 **Wyspecyfikowane wymaganie** – potrzeba lub oczekiwanie, które zostało określone

UWAGA do hasła: Wyspecyfikowane wymagania mogą być określone w dokumentach normatywnych, takich jak przepisy, normy i specyfikacje techniczne.

247 **Jednostka oceniająca zgodność** – jednostka wykonująca działania oceny zgodności, z wyłączeniem **akredytacji**

248 **Jednostka akredytująca** – jednostka wykonująca **akredytację**

249 Za każdym razem, gdy oceniane jest wymaganie, dokumentacja programu musi identyfikować następujące elementy:

(a) Rodzaj oceny zgodności. W kontekście programu certyfikacji Portfela EUDI jest to wybór spośród następujących: ocena i jej podtypy (badanie, audyt, inspekcja, walidacja, weryfikacja, certyfikacja (systemów zarządzania, produktu/usługi/procesu)), akredytacja.

(b) Uzasadnienie wyboru metody: z uwzględnieniem definicji metod i przepisów CIR (UE) 2024/2981.

A.2. Metody dotyczące oceny

250 *UWAGA: EN-ISO/IEC 17065 definiuje ogólne funkcje „Wybór” (Selection) i „Określanie” (Determination) w połączonym działaniu oceny zgodności zwanym „Oceną” (Evaluation).*

251 **Badanie** – określanie jednej lub większej liczby charakterystyk **przedmiotu oceny zgodności** według procedury

UWAGA: procedura to wyspecyfikowany sposób przeprowadzania działania lub procesu.

- 252 **Audyt** – proces uzyskiwania istotnych informacji o **przedmiocie oceny zgodności** i ich obiektywnej oceny w celu określenia stopnia, w jakim **wyspecyfikowane wymagania** zostały spełnione

UWAGA do hasła: Przykładami przedmiotów audytu są systemy zarządzania, procesy, produkty i usługi.

- 253 **Inspekcja** – badanie **przedmiotu oceny zgodności** i określenie jego zgodności ze szczegółowymi wymaganiami lub, na podstawie profesjonalnego osądu, z wymaganiami ogólnymi

UWAGA 1 do hasła: Badanie może obejmować obserwacje bezpośrednie lub pośrednie, które mogą obejmować pomiary lub dane wyjściowe przyrządów.

UWAGA 2 do hasła (zmodyfikowana): Programy oceny zgodności mogą określać inspekcję wyłącznie jako badanie.

- 254 **Walidacja** – potwierdzenie wiarygodności dla konkretnego zamierzonego użycia lub zastosowania poprzez dostarczenie obiektywnych dowodów, że **wyspecyfikowane wymagania** zostały spełnione

*UWAGA do hasła: Walidacja może być stosowana do **deklaracji (claims)** w celu potwierdzenia informacji zadeklarowanych w deklaracji dotyczącej zamierzonego przyszłego użycia.*

Zgodnie z EN ISO/IEC 17029 **deklaracja (claim)** to informacja zadeklarowana przez klienta.

- 255 **Weryfikacja** – potwierdzenie prawdziwości poprzez dostarczenie obiektywnych dowodów, że **wyspecyfikowane wymagania** zostały spełnione

*UWAGA do hasła: Weryfikacja może być stosowana do **deklaracji** w celu potwierdzenia informacji zadeklarowanych w deklaracji dotyczącej zdarzeń, które już nastąpiły, lub wyników, które już uzyskano.*

A.3. Różne rodzaje atestacji

- 256 **Atestacja** – wydanie stwierdzenia, na podstawie decyzji, że wykazano spełnienie *wyspecyfikowanych wymagań*

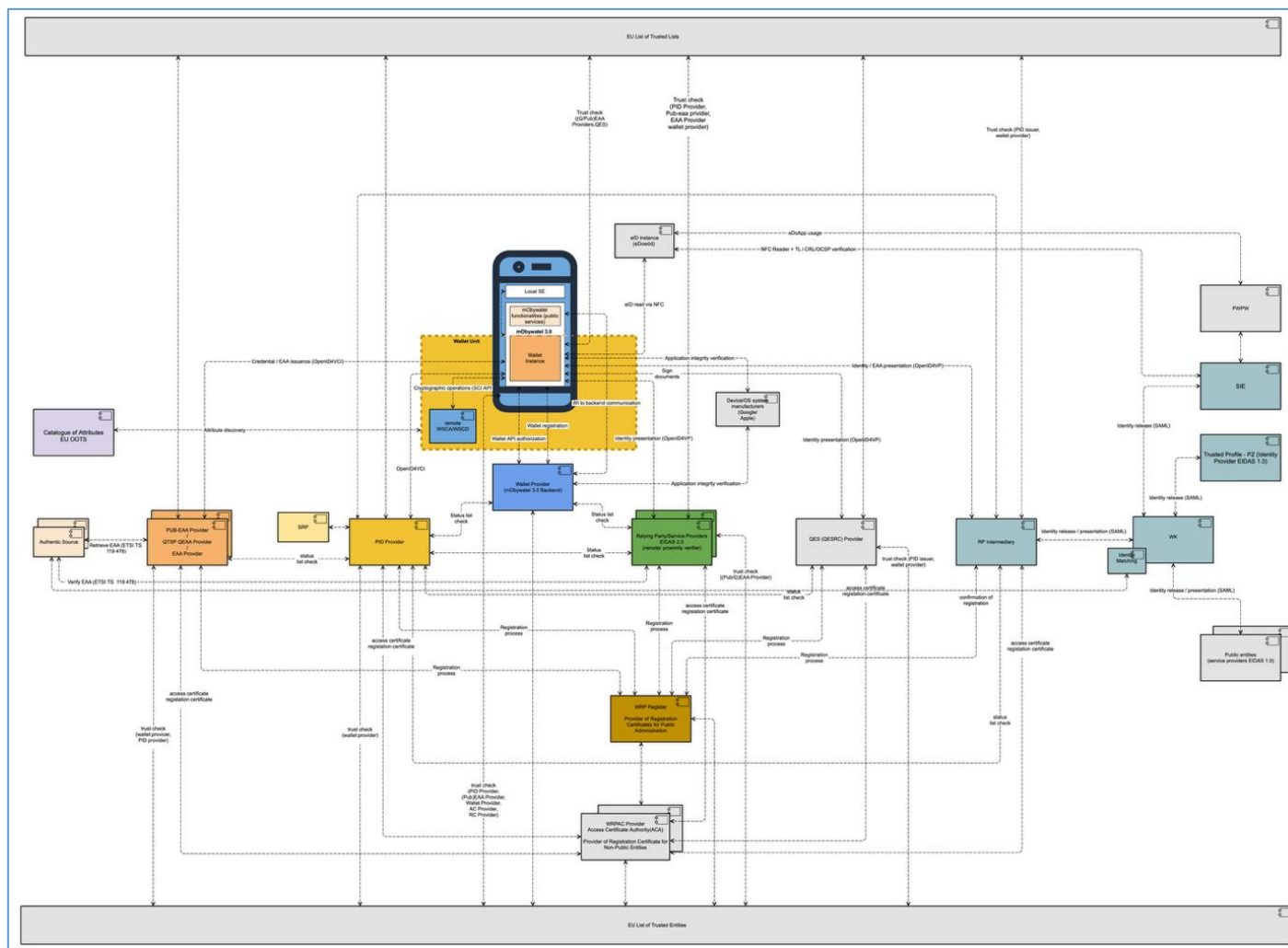
- 257 *UWAGA 1 do hasła (zmodyfikowana): Wynikające z tego stwierdzenie określa się mianem „stwierdzenia zgodności”.*

- 258 *UWAGA 2 do hasła (zmodyfikowana): Atestacja pierwszej strony jest nazywana **deklaracją (zgodności)**, natomiast atestację strony trzeciej rozróżnia się terminami **certyfikacja i akredytacja**.*
- 259 **Certyfikacja** – atestacja strony trzeciej dotycząca **przedmiotu oceny zgodności**, z wyjątkiem **akredytacji**
- 260 W programie certyfikacji Portfela EUDI stosuje się kilka przedmiotów certyfikacji, a mianowicie: systemy zarządzania, produkty, usługi i procesy.
- 261 Zgodnie z EN-ISO/IEC 17021-1, Wprowadzenie: Certyfikacja systemu zarządzania stanowi niezależne wykazanie, że system zarządzania organizacji:
- a) jest zgodny z wyspecyfikowanymi wymaganiami;
 - b) jest zdolny do konsekwentnego osiągnięcia deklarowanej polityki i celów;
 - c) jest skutecznie wdrożony.
- 262 Zgodnie z EN-ISO/IEC 17065, Wprowadzenie: Certyfikacja produktów, procesów lub usług jest środkiem zapewnienia, że są one zgodne z **wyspecyfikowanymi wymaganiami** zawartymi w normach i innych dokumentach normatywnych.
- 263 **Akredytacja** – atestacja strony trzeciej dotycząca **jednostki oceniającej zgodność**, stanowiąca formalne wykazanie jej kompetencji, bezstronności i spójnego działania w wykonywaniu określonych działań oceny zgodności.

Załącznik B Opis architektury rozwiązania portfela w Polsce

A. Diagram wysokopoziomowy rozwiązania Portfela EUDI w Polsce

Diagram przedstawiono na rysunku (Rysunek 6).



Rysunek 6 Wysokopoziomowa prezentacja rozwiązania Portfela EUDI w Polsce

B. Przegląd komponentów architektury

Nazwa komponentu	Typ komponentu	Opis komponentu	Łącze ARF / odniesienia prawne
mObywatel 3.0	Oprogramowanie	Aplikacja mobilna dla obywateli, zawierająca moduł Portfela i moduł Usług	N/A
Instancja portfela	Moduł oprogramowania	Moduł aplikacji mobilnej realizujący podstawowe funkcjonalności portfela	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#432-components-of-a-wallet-unit
Funkcjonalności mObywatel	Moduł oprogramowania	Moduł aplikacji mobilnej realizujący cyfrowy dostęp do usług publicznych (np. zamówienie paszportu, zastrzeżenia PESEL, ...). Powinien obejmować obecny zakres funkcjonalności mObywatel 2.0	N/A
Lokalny SE	Sprzęt	Odporny na manipulacje element bezpieczny (Secure Element) na urządzeniu lokalnym. Jeżeli jest dostępny – zawiera klucze do procesów autoryzacji i dostępu. Nie zawiera kluczy prywatnych użytkownika (te są przechowywane w elementach WSCA / WSCD)	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#432-components-of-a-wallet-unit
Jednostka portfela	Sprzęt / Oprogramowanie	Zbiór elementów: instancja portfela, WSCA, WSCD.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#432-components-of-a-wallet-unit
WSCA	Oprogramowanie	Aplikacja zarządzająca zasobami krytycznymi i zapewniająca operacje kryptograficzne dla instancji portfela. W obecnym rozwiązaniu zaimplementowana w modelu zdalnym WSCA / WSCD.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#432-components-of-a-wallet-unit
WSCD	Sprzęt	Do ochrony zasobów krytycznych używane są urządzenia odporne na manipulacje. W obecnym rozwiązaniu zaimplementowane w zdalnym modelu WSCA / WSCD jako urządzenie HSM zainstalowane w sieci dostawcy portfela.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#432-components-of-a-wallet-unit
Dostawca portfela (backend mObywatel 3.0)	Oprogramowanie / Podmiot	Usługi backendowe zapewniające funkcjonalności tworzenia obiektów portfela (takich jak WUA, WIA, ...) i zarządzania nimi	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#432-components-of-a-wallet-unit
Dostawca PID	Podmiot	Podmiot odpowiedzialny za weryfikację tożsamości użytkownika i wydawanie PID do jednostki portfela	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#34-person-identification-data-pid-providers
SRP (System Rejestrów Państwowych)	Oprogramowanie	Dane referencyjne (master data) tożsamości obywateli w Polsce. Wykorzystywany w procesach weryfikacji tożsamości (takich jak wydawanie PID)	N / A
Strona ufająca / dostawcy usług	Podmiot	Podmiot świadczący usługi dla użytkowników na podstawie atrybutów	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-

Nazwa komponentu	Typ komponentu	Opis komponentu	Łącze ARF / odniesienia prawne
		użytkownika zawartych w poświadczeniach (PID, EAA, PUB-EAA, ...)	framework/blob/main/docs/architecture-and-reference-framework-main.md#311-relying-parties-relying-party-instances-and-intermediaries
Producenci urządzeń / systemów operacyjnych (Google, Apple)	Podmiot	Firmy rozwijające systemy operacyjne na urządzeniach użytkowników i udostępniające API do weryfikacji integralności aplikacji i systemu operacyjnego	N / A
Instancja eID	Sprzęt	Fizyczny dokument tożsamości zawierający warstwy certyfikatów cyfrowych, umożliwiający weryfikację tożsamości użytkownika	N / A
PWPW (Polska Wytwórnia Papierów Wartościowych)	Podmiot	Podmiot dostarczający fizyczne dokumenty tożsamości, aplikację eDO App (aplikację cyfrowego dokumentu tożsamości) oraz funkcjonalności weryfikacji dokumentów tożsamości	N / A
SIE (System Identyfikacji Elektronicznej)	Oprogramowanie	Portal internetowy zapewniający funkcjonalności wydawania tożsamości użytkownika z fizycznego dokumentu tożsamości i/lub aplikacji eDO App	N / A
Profil Zaufany (Trusted Profile)	Oprogramowanie	System zapewniający funkcjonalności cyfrowej tożsamości użytkownika (np. wydawanie tożsamości, zarządzanie tożsamością, ograniczenia dostępu, ...)	N / A
WK (Węzeł Krajowy)	Oprogramowanie	System zapewniający procesy wydawania tożsamości. Integruje dostawców usług (prywatnych i publicznych) oraz źródła tożsamości	N / A
Identity Matching	Oprogramowanie	System zapewniający funkcjonalności transgranicznego dopasowywania tożsamości.	https://eur-lex.europa.eu/eli/reg_impl/2025/846/oj
Podmioty publiczne	Podmiot	Dostawcy usług eIDAS 1.0 wykorzystujący WK jako źródło tożsamości	N / A
Pośrednik RP	Podmiot	Podmiot działający w imieniu stron ufających. Często świadczy usługi techniczne dla wielu stron ufających, integrując się z jednostkami portfela oraz przetwarzając PID i inne poświadczenia.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#311-relying-parties-relying-party-instances-and-intermediaries
Dostawcy QES	Podmiot	Podmiot świadczący usługi podpisów i pieczęci cyfrowych dla użytkowników portfela.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#39-qualified-electronic-signature-remote-creation-qesrc-providers
Rejestrator WRP	Podmiot	Wydawca certyfikatów rejestracji dla podmiotów. Prowadzi rejestr podmiotów i ich certyfikatów w ekosystemie EUDI.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework-main.md#317-registrars
Rejestrator WRPAC	Podmiot	Wydawca certyfikatów dostępu dla podmiotów. Prowadzi rejestr podmiotów i ich certyfikatów w ekosystemie EUDI.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework-main.md#317-registrars https://github.com/eu-digital-identity-wallet/eudi-doc-

Nazwa komponentu	Typ komponentu	Opis komponentu	Łącze ARF / odniesienia prawne
			architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#318-access-certificate-authorities
Unijna lista zaufanych podmiotów	Podmiot	Podmiot zarządzający centralną listą wszystkich zaufanych podmiotów (np. dostawców portfeli, dostawców PID). Pełni rolę kotwicy zaufania w łańcuchu zaufania	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#35-trusted-list-or-lote-provider
Unijna lista list zaufania	Podmiot	Podmiot zarządzający listą list zaufania, które mogą być wykorzystywane do sprawdzania podmiotów, takich jak dostawcy QEAA i PuB-EAA	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#35-trusted-list-or-lote-provider
Dostawcy EAA (PUB-EAA, QEAA, EAA)	Podmiot	Zarejestrowane podmioty, które mogą wydawać elektroniczne poświadczenia atrybutów (EAA) do instancji portfela. Różne rodzaje dostawców EAA opisano w ARF.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#36-qualified-electronic-attestation-of-attributes-qeaa-providers https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#37-eaa-issued-by-or-on-behalf-of-a-public-sector-body-responsible-for-an-authentic-source-pub-eaa-providers https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework-main.md#38-non-qualified-electronic-attestation-of-attributes-eaa-providers
Źródło autentyczne	Oprogramowanie	Repozytoria (dane referencyjne) zawierające atrybuty użytkowników, wykorzystywane do tworzenia EAA (poświadczeń) na wniosek użytkownika za pośrednictwem dostawców EAA.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#310-authentic-sources
Katalog atrybutów EU OOTS	Oprogramowanie	Katalog umożliwiający podmiotom w ekosystemie EUDI zarządzanie schematami EAA, wyszukiwanie dostępnych EAA oraz walidację ich składni i semantyki.	https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#56-catalogue-of-attributes-and-catalogue-of-attestation-schemes