

GP-02

System Certyfikacji PL Portfela EUDI
Program certyfikacji cyberbezpieczeństwa

WERSJA 1.01

2026.07.09

Oznaczenie dokumentu	GP-02
Wersja	V1.01 (2026-07)
Status	FINAL
Data	09.07.2026
Rodzaj dokumentu	Program certyfikacji — specyfikacja programu (ISO/IEC 17067)
Ramy nadrzędne	G-01 System Certyfikacji PL Portfela EUDI G-02 Słownik G-03 Organizacja i wsparcie właściciela krajowego systemu certyfikacji EUDI G-04 Opracowanie i utrzymywanie rejestru ryzyk dla wdrażania i certyfikacji Portfela EUDI (projekt specyfikacji technicznej CEN) G-05 Wymagania akredytacyjne dla jednostek oceniających zgodność (CAB)
Właściciel programu	Rzeczpospolita Polska / Minister Cyfryzacji
Przedmiot certyfikacji	Cyberbezpieczeństwo Instancji Portfela EUDI
Odbiorcy pierwotni	Jednostki oceniające zgodność (CAB) akredytowane zgodnie z G-05
Odbiorcy wtórni	Dostawca Portfela EUDI
Poziom uzasadnienia zaufania <ocena>	Wysoki (rozporządzenie (UE) 2019/881)
Dokumenty podrzędne	Serie WP-02, WM-02

Historia zmian

Lp.	Zmiana	Wersja	Data
1.	Tłumaczenie wersji angielskiej	1.0	2026-07-08
2.	Poprawki edycyjne	1.01	2026-07-09

Spis treści

1	PRZEDMOWA.....	6
2	ZAKRES	7
3	PODSTAWA PRAWNA	8
4	POWOŁANIA.....	10
4.1	Normy i specyfikacje techniczne.....	10
4.2	Dokumenty nadrzędne	10
4.3	Dokumenty równorzędne.....	11
4.4	Dokumenty podrzędne.....	11
5	TERMINY I DEFINICJE	12
6	STRUKTURA PROGRAMU CERTYFIKACJI	13
6.1	Przedmiot certyfikacji	13
6.2	Role i odpowiedzialności.....	16
6.2.1	Przegląd interesariuszy programu	16
6.2.2	Akredytacja jednostek CAB.....	16
6.3	Mechanizmy zapewnienia bezstronności	17
6.4	Relacja do GP-01 i GP-03	17
6.5	Relacja do dokumentów podrzędnych WP-02 i WM-02	18
6.6	Typ programu	18
6.7	Korzystanie z certyfikacji i znaków zgodności	18
7	PROCESY OCENY I CERTYFIKACJI.....	19
7.1	Postanowienia ogólne.....	19
7.2	Faza przygotowania i wnioskowania	20
7.2.1	Diagram.....	20
7.2.2	Dokumentacja Wnioskodawcy.....	20
7.2.3	Formularz wniosku.....	21
7.3	Faza oceny	21
7.3.1	Spotkanie otwierające (kick-off).....	21
7.3.2	Ocena	22
7.3.3	Walidacja wyników oceny.....	24
7.3.4	Procedura jednorazowego rozszerzenia oceny	25
7.4	Faza certyfikacji.....	27
7.4.1	Diagram.....	27
7.4.2	Opis fazy.....	27
7.4.3	Dokumenty związane z certyfikacją	28
7.5	Pracochłonność oceny i certyfikacji.....	29
7.6	Postanowienia dodatkowe.....	29
8	UTRZYMANIE CERTYFIKATU	31

8.1	Postępowanie z niezgodnościami.....	31
8.2	Ogólne podejście do zarządzania zmianą	31
8.3	Zobowiązania posiadacza certyfikatu po certyfikacji	32
8.4	Ciągłość uzasadnienia zaufania w GP-02.....	32
8.4.1	Postanowienia ogólne	32
8.4.2	Ponowna ocena i ponowna certyfikacja.....	33
8.4.3	Zawieszenie lub cofnięcie certyfikatu	34
8.5	Nadzór.....	34
8.5.1	Coroczne działania w nadzorze.....	34
8.5.2	Wynik nadzoru.....	35
8.6	Skutki zmian certyfikatów GP-01 / GP-03	36
9	POSTANOWIENIA KOŃCOWE	37
9.1	Ustawodawstwo krajowe.....	37
9.2	Umowy o ocenę i certyfikację	37
9.3	Koszty	37
	ZAŁĄCZNIKI	38

1 **Przedmowa**

- 1 Niniejszy dokument (GP-02) przedstawia specyfikację programu certyfikacji cyberbezpieczeństwa, jednego z trzech programów certyfikacji w ramach Systemu Certyfikacji PL EUDIW ustanowionego przez Rzeczpospolitą Polską. Określa on program certyfikacji — w rozumieniu PN-EN ISO/IEC 17067 — który akredytowane jednostki certyfikujące (CAB) stosują przy certyfikacji cech cyberbezpieczeństwa właściwego produktu ICT lub jego komponentów, w ramach których dostarczane jest rozwiązanie Europejskiego Portfela Tożsamości Cyfrowej (EUDI Wallet).
- 2 Proces certyfikacji o ustalonym czasie trwania stanowi racjonalne podejście do certyfikacji rozwiązania Portfela EUDI.
- 3 Celem GP-02 jest skrócenie czasu trwania procedur i wdrożenie efektywniejszego harmonogramu poprzez unikanie nadmiernych formalności i pętli komunikacyjnych oraz koncentrację na ocenach wykonywanych przez wysoko wykwalifikowanych oceniających.
- 4 GP-02 jest adresowany przede wszystkim do CAB prowadzących działania certyfikacyjne w ramach programu certyfikacji cyberbezpieczeństwa. Dostawcy rozwiązania Portfela EUDI powinni czytać niniejszy dokument łącznie z mającymi zastosowanie dokumentami podrzędnymi serii WP-02, które określają wymagania merytoryczne, jakie mają oni spełnić.
- 5 Niniejszy dokument stanowi część serii GP, funkcjonującej w ramach nadzoru ustanowionych przez serię G (Ramy programu). Należy go czytać łącznie z G-01 (System certyfikacji PL portfela EUDI) oraz G-03 (Organizacja i wsparcie dla właściciela krajowego programu certyfikacji EUDI).

2 Zakres

- 6 Dokument określa program certyfikacji cyberbezpieczeństwa rozwiązania Europejskiego Portfela Tożsamości Cyfrowej, dostarczanego przez Rzeczpospolitą Polską, w ramach Systemu Certyfikacji PL Portfela EUDI.
- 7 GP-02 ustanawia wymagania dotyczące produktu (przez odesłanie do dokumentów podrzędnych), mające zastosowanie metodyki oceny (przez odesłanie do dokumentów podrzędnych i norm) oraz procedury oceny zgodności, które akredytowane jednostki CAB stosują przy ocenie i certyfikacji w ramach programu cyberbezpieczeństwa, a także dostawców produktów i usług działających w jego ramach. Dokument jest przeznaczony do czytania łącznie z G-05, który określa wymagania akredytacyjne wobec samych jednostek oceniających zgodność.

3 Podstawa prawna

8 Program certyfikacji określony w niniejszym dokumencie jest ustanowiony na podstawie następujących aktów prawnych:

- Rozporządzenie (UE) 910/2014, w szczególności art. 5a i 5c.
- Rozporządzenie (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych.
- Rozporządzenie wykonawcze Komisji (UE) 2024/2981 z dnia 28 listopada 2024 r. w sprawie certyfikacji europejskich portfeli tożsamości cyfrowej, w szczególności art. 3–5, 8, 12–14 i 19 oraz załączniki I–VII.
- Rozporządzenie wykonawcze Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. w sprawie integralności i podstawowych funkcjonalności europejskich portfeli tożsamości cyfrowej.
- Rozporządzenie wykonawcze Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie danych identyfikujących osobę wydawanych do europejskich portfeli tożsamości cyfrowej.
- Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie poziomów bezpieczeństwa środków identyfikacji elektronicznej.
- Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. w sprawie środków zarządzania ryzykiem w cyberbezpieczeństwie.
- Rozporządzenie (UE) nr 765/2008 w sprawie akredytacji i nadzoru rynku, w szczególności art. 4 i 5.
- Rozporządzenie wykonawcze Komisji (UE) 2026/798 z dnia 7 kwietnia 2026 r. ustanawiające zasady stosowania rozporządzenia (UE) nr 910/2014 w odniesieniu do norm odniesienia i specyfikacji dotyczących zdalnego onboardingu użytkowników europejskich portfeli tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej odpowiadających poziomowi bezpieczeństwa „znaczny” w połączeniu z dodatkowymi procedurami zdalnego onboardingu, gdy takie połączenie spełnia wymagania poziomu bezpieczeństwa „wysoki”.
- Ustawa o usługach zaufania oraz identyfikacji elektronicznej.

- Ustawa o aplikacji mObywatel.
- Ustawa o krajowym systemie cyberbezpieczeństwa.

4 Powołania

4.1 Normy i specyfikacje techniczne

- | | |
|----|---|
| 9 | PN-EN ISO/IEC 17065, Ocena zgodności — Wymagania dla jednostek certyfikujących wyroby, procesy i usługi |
| 10 | PN-EN ISO/IEC 17067, Ocena zgodności — Podstawy certyfikacji wyrobów oraz wytyczne dotyczące programów certyfikacji wyrobów |
| 11 | PN-EN ISO/IEC 17025, Ocena zgodności — Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących |
| 12 | PN-EN ISO/IEC 17007, Ocena zgodności — Wytyczne dotyczące redagowania dokumentów normatywnych odpowiednich do stosowania w ocenie zgodności |
| 13 | PN-EN ISO/IEC 17000:2020, Ocena zgodności — Terminologia i zasady ogólne |
| 14 | PN-EN ISO/IEC 15408:2023 (wieloarkuszowa), Kryteria oceny zabezpieczeń informatycznych |
| 15 | PN-EN ISO/IEC 18045:2023, Kryteria oceny zabezpieczeń informatycznych — Metodyka oceny zabezpieczeń informatycznych |
| 16 | PN-EN 17640:2022+A1:2026, Metodyka oceny cyberbezpieczeństwa o ustalonym czasie trwania dla produktów ICT (FITCEM) |

4.2 Dokumenty nadrzędne

- | | |
|----|---|
| 17 | G-01. System Certyfikacji PL Portfela EUDI |
| 18 | G-02. Słownik |
| 19 | G-03. Organizacja i wsparcie właściciela krajowego systemu certyfikacji EUDI |
| 20 | G-04. Opracowanie i utrzymywanie rejestru ryzyk dla wdrażania i certyfikacji Portfela EUDI (projekt specyfikacji technicznej CEN) |
| 21 | G-05. Wymagania akredytacyjne dla jednostek oceny zgodności (CAB) |

4.3 Dokumenty równorzędne

22 GP-01. Program certyfikacji funkcjonalnej Portfela EUDI

23 GP-03. Program certyfikacji eID

4.4 Dokumenty podrzędne

24 WP-02-01. Dekompozycja — wymagania bezpieczeństwa Portfela EUDI

25 WP-02-02. Profil zabezpieczeń FITCEM dla aplikacji — Instancja Portfela EUDI

26 WM-02-01. Rozszerzenie metodyki FITCEM na Rozwiązanie Portfela EUDI

27 WM-02-02. Adaptacja metodyki ewaluacji zgodnej z CEM dla komponentu WSCA

5 Terminy i definicje

28 Dla potrzeb niniejszego dokumentu wszystkie terminy i definicje podano w G-02. Słownik.

29 Dodatkowo stosuje się terminy i definicje z:

- rozporządzenia wykonawczego Komisji (UE) 2024/482,
- PN-EN 17640:2022 + A1:2026,

oraz następujące.

30 Raport analizy wpływu (Impact Analysis Report, IAR) — dokument rejestrujący analizę wpływu zmian na certyfikowany produkt ICT

31 *UWAGA 1 do hasła: IAR odnosi się do zmian certyfikowanego przedmiotu certyfikacji określonego w niniejszym dokumencie.*

6 Struktura programu certyfikacji

32 UWAGA: W niniejszym rozdziale przedstawiono wyłącznie te elementy struktury, które są specyficzne dla GP-02. Postanowienia ogólne zawarto w G-01.

6.1 Przedmiot certyfikacji

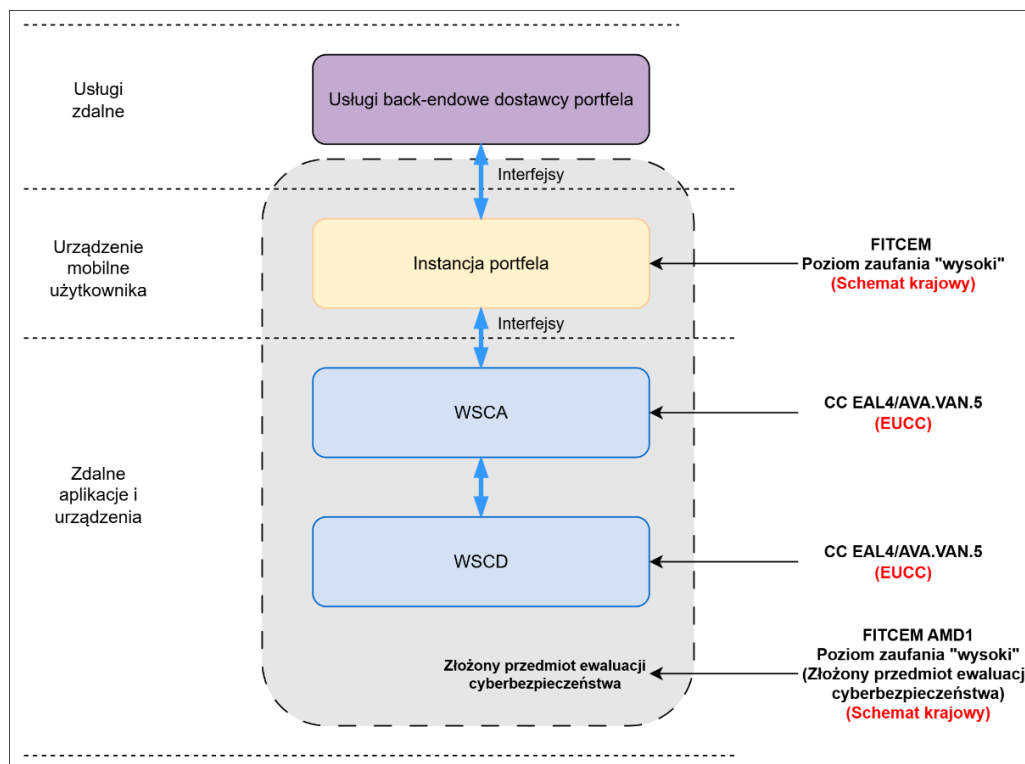
33 Przedmiotem certyfikacji w ramach niniejszego programu jest złożony przedmiot oceny (composite TOE) zgodnie z EN 17640:2022+A1:2026.

34 Złożony TOE składa się z następujących komponentów i interfejsów (patrz Tabela 1)

Tabela 1 Złożony TOE

Elementy TOE	Akronim komponentu	Program certyfikacji
bezpieczne urządzenie kryptograficzne portfela (Wallet Secure Cryptographic Device)	WSCD	EUCC
bezpieczna aplikacja kryptograficzna portfela (Wallet Secure Cryptographic Application)	WSCA	EUCC
instancja portfela (Wallet Instance)	WI	GP-02
interfejsy WI	nie dot.	GP-02

35 Zgodnie z rozporządzeniem 910/2014 oraz rozporządzeniem wykonawczym Komisji 2024/2981 niektóre komponenty złożonego TOE, tj. WSCD i WSCA, podlegają ocenie i następnie certyfikacji w ramach europejskiego programu certyfikacji cyberbezpieczeństwa (EUCC), patrz Rysunek 1.



Rysunek 1 Złożony TOE

- 36 W odniesieniu do wyników oceny i następnie certyfikacji WSCD/WSCA, właściwe interfejsy TOE do WSCA podlegają ocenie w ramach GP-02.
- 37 Zwięzłe informacje o interfejsach WI podano w Tabeli 2.
- 38 *UWAGA 1: Wszystkie informacje o interfejsach przygotowano na podstawie ARF v2.8.0.*
- 39 *UWAGA 2: Elementy, które nie zostały opisane w ARF, oznaczono kolorem żółtym.*

Tabela 2 Interfejsy WI

Lp.	Komponent lub podmiot komunikujący się z WI	Funkcjonalność wspierana przez protokół	Protokół	Kto wywołuje	Nazwa w ARF	Uwagi
1	Backend Dostawcy Portfela	rejestracja WI, weryfikacja WI	Niestandardowy przepływ komunikacji z użyciem REST API (oparty na HTTP, TLSv1.3)	WI	Interfejs Dostawcy Portfela	ARF 4.3.3: Ponieważ Dostawca Portfela odpowiada za obie strony tego interfejsu, nie będzie on definiowany ani standaryzowany w ramach ekosystemu Portfela EUDI.

Lp.	Komponent lub podmiot komunikujący się z WI	Funkcjonalność wspierana przez protokół	Protokół	Kto wywołuje	Nazwa w ARF	Uwagi
		wydawanie WUA, wydawanie WIA, utrzymanie poświadczeń	Niestandardowy przepływ komunikacji z użyciem REST API (oparty na HTTP, TLSv1.3)	WI	Interfejs Dostawcy Portfela	ARF 4.3.3: Ponieważ Dostawca Portfela odpowiada za obie strony tego interfejsu, nie będzie on definiowany ani standaryzowany w ramach ekosystemu Portfela EUDI.
2	WSCA	operacje kryptograficzne z użyciem WSCD	Niestandardowy przepływ komunikacji z użyciem REST API (oparty na HTTP, TLSv1.3)	WI	Bezpieczny Interfejs Kryptograficzny	ARF 4.3.3: W przypadku gdy WSCA jest dostarczana przez Dostawcę Portfela, Dostawca Portfela odpowiada za obie strony tego interfejsu, w związku z czym standaryzacja nie jest potrzebna w ramach ekosystemu Portfela EUDI.
3	Platformy (iOS, Android)	weryfikacja urządzenia użytkownika, weryfikacja bezpieczeństwa aplikacji	-	WI	-	Nie zdefiniowano w ARF v2.8.0
4	Użytkownik	interakcja z użytkownikiem	N/D — interfejs pomiędzy użytkownikiem a instancją portfela	Użytkownik	Interfejs Użytkownika	ARF 4.3.3: Ten interfejs nie będzie standaryzowany w ramach ekosystemu Portfela EUDI.
5	Strona ufająca	zdalne interakcje pomiędzy RP a WI	OpenID4VP + W3C Digital Credentials API (protokół standardowy)	Strona ufająca	Interfejs Prezentacji	
		interakcje bliskiego zasięgu pomiędzy RP a WI	ISO/IEC 18013-5 (protokół standardowy)	Strona ufająca	Interfejs Prezentacji	
6	Dostawcy poświadczeń	żądanie i odbieranie PID od dostawców PID	OpenID4VCI (protokół standardowy)	WI	Interfejs Wydawania PID	
		żądanie i odbieranie poświadczeń od dostawców poświadczeń	OpenID4VCI (protokół standardowy)	WI	Interfejs Wydawania Poświadczeń	
7	Dostawcy QESRC	zdalne generowanie kwalifikowanego podpisu elektronicznego i podpisywanie dokumentów	Nie zdefiniowano w ARF v2.8.0	WI	Interfejs Zdalnego Podpisywania lub Pieczętowania	Komponent opcjonalny w ARF v2.8.0
8	Magazyn kluczy	przechowywanie niekrytycznych zasobów kryptograficznych	-	WI	- (w ramach urządzenia użytkownika)	1. Komponent opcjonalny w ARF v2.8.0 2. Interfejs nie będzie standaryzowany w ramach ekosystemu Portfela EUDI
9	QSCD	lokalne podpisywanie dokumentów z użyciem kwalifikowanego podpisu elektronicznego	-	WI	- (w ramach urządzenia użytkownika)	1. Komponent opcjonalny w ARF v2.8.0 2. Interfejs nie będzie standaryzowany w ramach ekosystemu Portfela EUDI

6.2 Role i odpowiedzialności

6.2.1 Przegląd interesariuszy programu

40 Przegląd ról i odpowiedzialności przedstawiono w Tabeli 3.

Tabela 3 Przegląd ról i odpowiedzialności

Rola	Odpowiedzialności	Podstawa normatywna
Właściciel programu	Jest właścicielem programu i sprawuje nad nim nadzór; upoważnia jednostki CAB; prowadzi rejestr certyfikatów; monitoruje program.	PN-EN ISO/IEC 17067
CAB-CB	Zarządza procesem certyfikacji; prowadzi program certyfikacji poprzez wydawanie i utrzymywanie certyfikatów; wydaje wiążące wytyczne dla CAB-ITSEF.	PN-EN ISO/IEC 17065:2012
CAB-ITSEF¹	Wykonuje ocenę FITCEM.	PN-EN ISO/IEC 17025; EN 17640:2022+A1:2026
Wnioskodawca	Zgłasza produkt do certyfikacji; dostarcza dowody do oceny; przestrzega zobowiązań po certyfikacji.	GP-02
Krajowa jednostka akredytująca (NAB)	Akredytuje CAB-CB (EN ISO/IEC 17065) oraz CAB-ITSEF (EN ISO/IEC 17025) we właściwym zakresie.	[REG 2008/765]; G-05
Organy nadzoru rynku	Nadzór nad certyfikowanymi produktami na rynku. Rolę tę będzie pełnił Właściciel programu.	PN-EN ISO/IEC 17067; GP-02

6.2.2 Akredytacja jednostek CAB

- 41 Jednostki CAB-CB działające w ramach niniejszego programu są akredytowane przez krajową jednostkę akredytującą zgodnie z PN-EN ISO/IEC 17065:2012, w zakresie obejmującym rozwiązanie Portfela EUDI na poziomie uzasadnienia zaufania „wysoki”, zgodnie z [REG CSA].
- 42 Wymagane kompetencje CAB-CB określono w G-05.
- 43 Działalność CAB-ITSEF podlega akredytacji przez krajową jednostkę akredytującą zgodnie z PN-EN ISO/IEC 17025, w zakresie obejmującym

¹ CAB-ITSEF wykonuje ocenę WSCA w ramach programu EUCC

rozwiązanie Portfela EUDI na poziomie uzasadnienia zaufania „wysoki”, zgodnie z [REG CSA].

44 Wymagane kompetencje CAB-ITSEF określono w G-05.

6.3 Mechanizmy zapewnienia bezstronności

45 CAB-CB jest zobowiązana wdrożyć mechanizm zapewnienia bezstronności zgodnie z EN ISO/IEC 17065. Bezstronność jest gwarantowana poprzez następujący mechanizm w procesie certyfikacji o ustalonym czasie trwania:

- deklaracje bezstronności są składane przez certyfikujących przed rozpoczęciem procesu,
- regularne wyrywkowe audyty proceduralne prowadzone przez Właściciela programu,
- zarządzanie jakością w celu stałego badania potencjalnych przesłanek stronniczości i wywierania wpływu.

46 Te same środki podejmowane w celu zapewnienia bezstronności wdraża CAB-ITSEF, co stanowi uzupełnienie odpowiednich przepisów normy PN-EN ISO/IEC 17025.

6.4 Relacja do GP-01 i GP-03

47 GP-02 jest jednym z trzech programów certyfikacji w ramach Systemu Certyfikacji PL EUDIW. Seria GP-01 (Program certyfikacji funkcjonalnej EUDI) dotyczy zgodności funkcjonalnej aplikacji mobilnej portfela; seria GP-03 (Program certyfikacji cyberbezpieczeństwa eID) dotyczy certyfikacji usług i procesów związanych z Portfelem EUDI. Te programy certyfikacji określają wymagania oceniane i certyfikowane niezależnie od GP-02, jednak wynikające z nich certyfikaty traktuje się jako podstawę wydania certyfikatu najwyższego poziomu, o którym mowa w rozporządzeniu 910/2014, art. 5c, G-01 oraz zgodnie z procedurą powiązania określoną w GP-03.

48 W przypadku zawieszenia, cofnięcia lub wygaśnięcia certyfikatu GP-01 lub GP-03 Dostawca EUDI powiadamia bez zbędnej zwłoki Właściciela Systemu PL Portfela EUDI oraz właściwe jednostki CAB działające w ramach GP-02. Skutki dla certyfikatów / deklaracji zgodności GP-02 uregulowano w G-01, sekcja 5.3.

6.5 Relacja do dokumentów podrzędnych WP-02 i WM-02

- 49 Dokumenty podrzędne serii WP-02 i serii WM-02 stanowią treść normatywną programu certyfikacji cyberbezpieczeństwa. Określają one odpowiednio:
- 50 WP-02-01. Dekompozycja — wymagania bezpieczeństwa Portfela EUDI — dokument określa wymagania bezpieczeństwa wywiedzione z rozporządzeń wykonawczych i oparte na właściwych normach EN lub ich projektach, albo na powszechnie uznanych rozwiązaniach typu „dobra praktyka”.
- 51 WP-02-02. Profil zabezpieczeń FITCEM dla aplikacji — Instancja Portfela EUDI — dokument określa profil zabezpieczeń zgodnie z PN-EN 17640 i zawiera szczegółowe wskazówki dotyczące dokumentu Security Target.
- 52 WM-02-01. Rozszerzenie metodyki FITCEM na Jednostkę/Rozwiązanie Portfela EUDI —obejmuje uzasadnienie zastosowania poziomu uzasadnienia zaufania „wysoki” do oceny rozwiązania Portfela EUDI oraz wytyczne dotyczące przeprowadzania rozszerzonej kryptoanalizy wskazanej w normie PN-EN 17640.

6.6 Typ programu

- 53 Niniejszy program certyfikacji odpowiada modelowi typu 5 zdefiniowanemu w ISO/IEC 17067, obejmującemu wstępne badania i ocenę, nadzór nad wyrobem oraz ponowną ocenę / ponowną certyfikację. Program określa elementy wymienione w rozdziale 6.5 PN-EN ISO/IEC 17067, zgodnie z art. 4 ust. 3 lit. a) rozporządzeniem wykonawczym Komisji (UE) 2024/2981.

6.7 Korzystanie z certyfikacji i znaków zgodności

- 54 Jako znak zgodności dla certyfikacji wydawanych w ramach niniejszego programu stosuje się wyłącznie znak zgodności PL Portfela EUDI zdefiniowany w G-03.
- 55 Wspólne wymagania dotyczące korzystania z certyfikacji i znaków zgodności określono w G-01 i G-03.
- 56 CAB-CB odpowiada za przyznawanie, zawieszanie i cofanie prawa do używania znaku zgodności stosownie do decyzji certyfikacyjnych podejmowanych przez nią w ramach niniejszego programu. W przypadku zawieszenia lub cofnięcia certyfikatu Dostawca Portfela EUDI zaprzestaje używania znaku zgodności bez zbędnej zwłoki.

7 Procesy oceny i certyfikacji

7.1 Postanowienia ogólne

- 57 EN 17640/AMD1 stosuje się do rozwiązania Portfela EUDI na poziomie uzasadnienia zaufania „wysoki”, zgodnie z [REG CSA]. W związku z tym zestaw zadań oceny przedstawiono w Tabeli 4.

Tabela 4 Wymagania dotyczące uzasadnienia zaufania stosowane w ocenie

Wymaganie podlegające ocenie	Odesłanie do EN 17640:2022+A1:2 026	Poziom uzasadnienia zaufania: wysoki
Kontrola kompletności	6.1	Wymagane
Przegląd funkcjonalności bezpieczeństwa	6.3	Wymagane
Ocena FIT Security Target	6.4	Wymagane
Dokumentacja wytworzenia	6.5	Wymagane
Ocena instalacji TOE	6.6	Wymagane
Testy zgodności	6.7	Wymagane
Testy podatności	6.9	Wymagane
Testy penetracyjne	6.10	Wymagane
Rozszerzona analiza kryptograficzna	6.12	Wymagane
Ocena złożonego TOE (kompozycji)	6.13	Wymagane

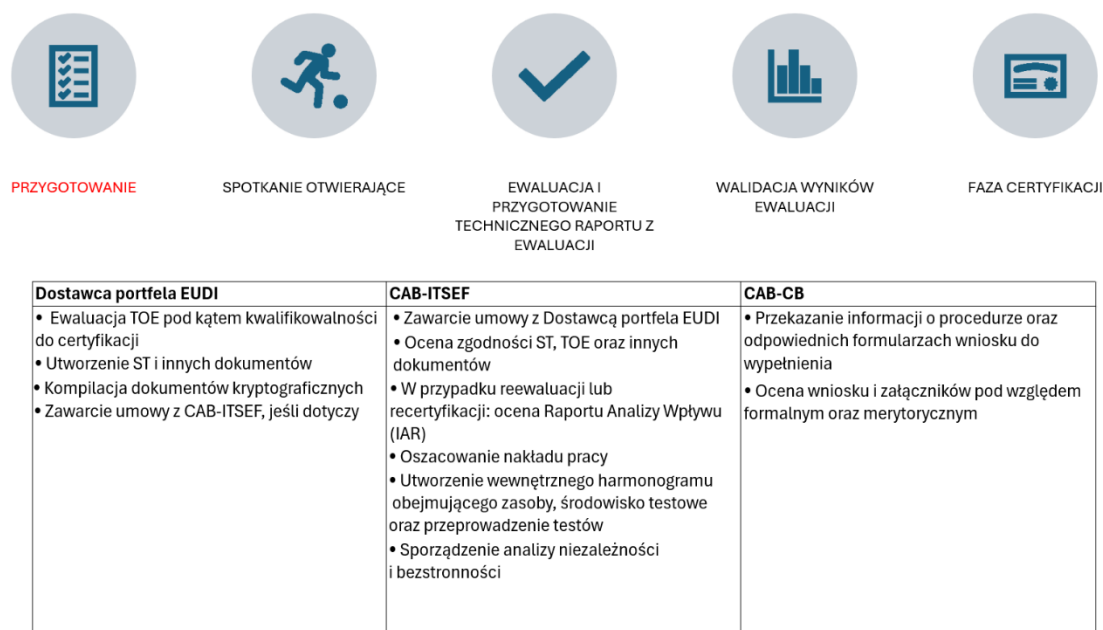
- 58 Proces certyfikacji GP-02 dzieli się na trzy fazy obejmujące łącznie pięć kroków procesowych:
- faza przygotowania i wnioskowania,
 - faza oceny:
 1. spotkanie otwierające (kick-off),
 2. ocena i przygotowanie technicznego raportu z oceny,
 3. walidacja wyników oceny,
 - faza certyfikacji.

7.2 Faza przygotowania i wnioskowania

59 UWAGA: faza odzwierciedla PN-EN ISO/IEC 17065, 7.2 i 7.3.

7.2.1 Diagram

60 Zadania właściwych ról w tej fazie przedstawiono na Rysunek 2.



Rysunek 2 . Prezentacja fazy przygotowania

7.2.2 Dokumentacja Wnioskodawcy

61 Od Wnioskodawcy wymagane są następujące dokumenty i informacje:

- dokument Security Target (ST) — zadanie zabezpieczeń (patrz GP-02/Załącznik A),
- skrótowy przegląd architektury (np. system operacyjny, centralne komponenty oprogramowania),
- wykaz komponentów oprogramowania (software bill of materials, SBOM) (patrz GP-02/Załącznik C),
- zwięzłe techniczne objaśnienie procedury aktualizacji,
- dokumentacja kodu źródłowego wymagana do kryptoanalizy zgodnie z załącznikiem (GP-02/Załącznik D),
- wykaz ogólnie potwierdzający zgodność z poszczególnymi wymaganiami minimalnymi we właściwym zakresie,

- bezpieczny przewodnik użytkownika (Secure User Guide, SUG), zapewniający, że TOE znajduje się w stanie umożliwiającym certyfikację. SUG (patrz GP-02/Załącznik B) dołącza się do TOE w przypadku pomyślnej certyfikacji,
- kod źródłowy aplikacji wraz z informacją o ścieżce kompilacji użytej do wygenerowania TOE.

7.2.3 Formularz wniosku

- 62 Formularz wniosku zawiera informacje wymagane do rozpoczęcia i przeprowadzenia procedury.
- 63 Formularz wniosku jest przygotowywany i dystrybuowany zgodnie z procedurami wewnętrznymi CAB-CB oraz zawiera wyjaśnienia i instrukcje pomocne przy jego wypełnianiu.
- 64 Wnioskodawca może złożyć formularz wniosku w ramach GP-02 odrębnie albo formularz łączony, odpowiednio do programu certyfikacji GP-01 w ramach Systemu Certyfikacji PL Portfela EUDI.

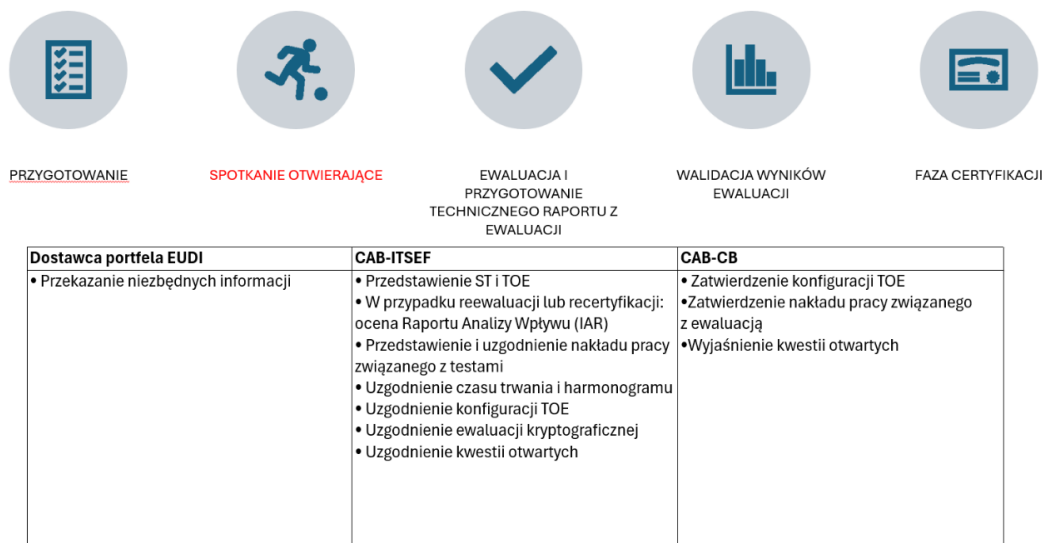
7.3 Faza oceny

- 65 *UWAGA: faza odzwierciedla PN-EN ISO/IEC 17065, 7.4 i 7.5.*

7.3.1 Spotkanie otwierające (kick-off)

7.3.1.1 Diagram

- 66 Zadania właściwych ról w tej podfazie przedstawiono na Rysunek 3.



Rysunek 3 Prezentacja podfazy spotkania otwierającego

7.3.1.2 Opis fazy

67 Spotkanie otwierające odbywa się nie później niż 5 dni roboczych po otrzymaniu przez CAB-CB dokumentu Security Target oraz wszystkich pozostałych dokumentów Wnioskodawcy.

68 W spotkaniu uczestniczą wszystkie strony zaangażowane w procedurę, tj. Wnioskodawca, CAB-ITSEF i CAB-CB.

7.3.2 Ocena

7.3.2.1 Diagram

69 Zadania właściwych ról w tej podfazie przedstawiono na Rysunek 4.



Rysunek 4 Prezentacja fazy oceny

7.3.2.2 Opis fazy

- 70 Ocenę przeprowadza się zgodnie ze specyfikacjami zawartymi w sekcji 7.1 niniejszego dokumentu.
- 71 W tym czasie CAB-ITSEF nie wolno uzgadniać z Wnioskodawcą ani producentem swojej oceny wykrytych podatności.
- 72 Komunikacja między zainteresowanymi stronami w trakcie oceny jest dozwolona lub wymagana w następujących sytuacjach:
- CAB-ITSEF może, w razie potrzeby, żądać od Wnioskodawcy informacji w kwestiach technicznych na potrzeby oceny.
 - CAB-ITSEF może informować Wnioskodawcę o wszelkich odchyleniach od uzgodnionego harmonogramu. Pozostałe zainteresowane strony są niezwłocznie powiadamiane o wszelkich opóźnieniach powstałych w uzgodnionym harmonogramie.
 - CAB-ITSEF powiadamia CAB-CB o wszelkich istotnych ustaleniach. Po zbadaniu ustaleń CAB-CB podejmuje decyzję, czy poinformować Wnioskodawcę samodzielnie, czy zażądać, aby uczyniła to CAB-ITSEF.
- 73 Ustalenie uznaje się za istotne, jeżeli spełnia co najmniej jedno z następujących kryteriów:

- CAB-ITSEF uznaje, że ustalenie stanowi znaczące ryzyko bezpieczeństwa z realistycznymi scenariuszami ataku dla produktu, który jest już dostępny w sprzedaży lub w użyciu albo będzie w najbliższej przyszłości.
- CAB-ITSEF uznaje, że ustalenie stanowi znaczące odchylenie lub podatność, które uniemożliwiłyby certyfikację, i że w produkcji należy w związku z tym wprowadzić istotne zmiany.

74 UWAGA: Istotne spostrzeżenie jest uznawane za niezgodność.

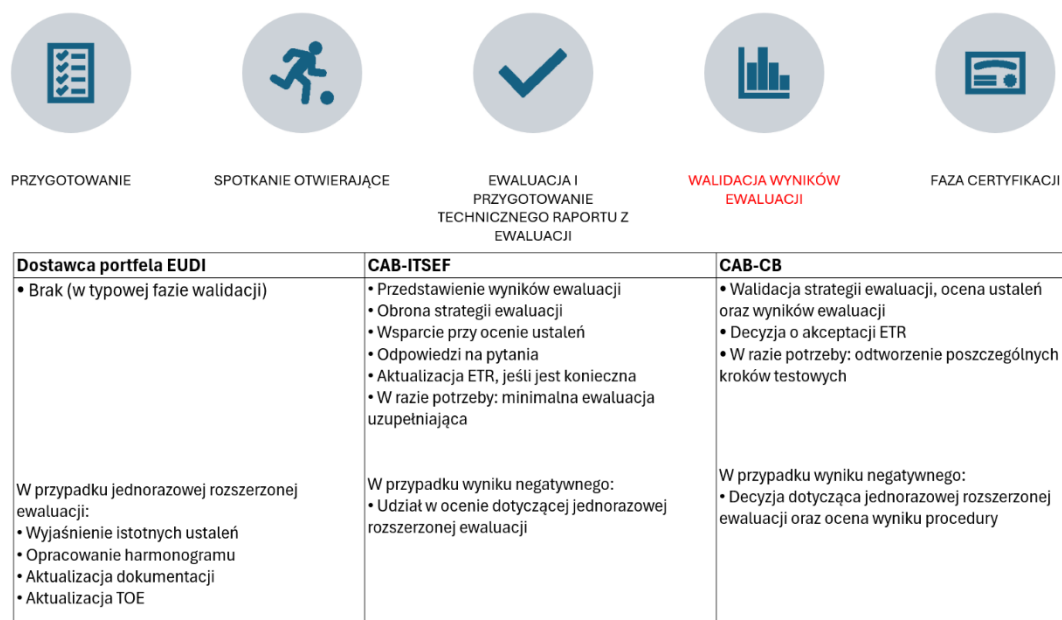
75 CAB-ITSEF dokumentuje potrzebę dodatkowych informacji zidentyfikowaną podczas oceny, błędy i niespójności w przedłożonych dokumentach oraz podatności i odchylenia zidentyfikowane w TOE. Wszystkie istotne informacje zamieszcza się w technicznym raporcie z oceny (Evaluation Technical Report, ETR).

76 Dodatkowo, ETR zawiera ogólną ocenę, w tym opinię w sprawie certyfikacji.

7.3.3 Walidacja wyników oceny

7.3.3.1 Diagram

81 Zadania właściwych ról w tej podfazie przedstawiono na Rysunek 5.



Rysunek 5 Prezentacja podfazy walidacji

7.3.3.2 Opis fazy

- 77 CAB-ITSEF przesyła ETR do CAB-CB w celu przeglądu, korzystając z bezpiecznego kanału komunikacji.
- 78 CAB-CB organizuje spotkanie z CAB-ITSEF, na którym CAB-ITSEF przedstawia swoje podejście, strategię badań oraz wyniki oceny.
- 79 CAB-CB przeprowadza szczegółową ocenę tych wyników w celu ustalenia, czy przeprowadzona ocena jest wystarczająca do końcowej oceny przedmiotu oceny (TOE).
- 80 Jeżeli podczas walidacji CAB-CB zidentyfikuje pozostałe kwestie otwarte, które można wyjaśnić w drodze dodatkowych badań o niewielkiej pracochłonności, może zażądać ich wykonania przez CAB-ITSEF. Zakres testów dodatkowych jest ograniczony i testy te przeprowadza się tylko wtedy, gdy są niezbędne do podjęcia decyzji certyfikacyjnej.
- 81 W celu adekwatnej odpowiedzi na kwestie otwarte może zostać zaangażowany Wnioskodawca, który dostarcza istotne informacje. Może to obejmować informacje o produkcie lub udostępnienie środowiska testowego.
- 82 Jeżeli decyzja certyfikacyjna dla TOE jest negatywna, CAB-CB — w porozumieniu z CAB-ITSEF — może zaproponować Wnioskodawcy jednorazowe rozszerzenie oceny, opisane w sekcji 7.3.4.

7.3.4 Procedura jednorazowego rozszerzenia oceny

- 83 Procedurę można zastosować wyłącznie wtedy, gdy CAB-CB uznaje TOE za zasadniczo gotowy do certyfikacji.
- 84 W ramach tej procedury Wnioskodawca może bezpośrednio odnieść się do ustaleń zidentyfikowanych przez CAB-ITSEF podczas oceny, wprowadzając ograniczone zmiany we właściwym TOE przedstawionym w procedurze pierwotnej.
- 85 Kryteria otwarcia jednorazowego rozszerzenia oceny są następujące:
- Ocena przeprowadzona przez ITSEF zakończyła się konkretnymi ustaleniami, które implikują bezpośrednie zmiany w TOE.

- Oszacowania pracochłonności dokonuje CAB-ITSEF na podstawie pierwotnego oszacowania dla TOE. Co do zasady nie może ona przekroczyć jednej trzeciej pierwotnej pracochłonności oceny.
- CAB-ITSEF jest w stanie zapewnić niezbędny czas i zasoby kadrowe na jednorazowo rozszerzoną ocenę.
- Łączny wymagany zakres zmian TOE jest jednoznacznie definiowalny, tj. zmiany w TOE dotyczą wyłącznie objętych ustaleniami elementów i wynikających z nich zależności.

- 86 Jeżeli kryteria są spełnione, CAB-CB przesyła Wnioskodawcy żądanie ponownego przedłożenia poprawionego TOE, co może obejmować zarówno sprzęt, jak i oprogramowanie, a także właściwą dokumentację (np. ST, SUG).
- 87 Wnioskodawca przedkłada CAB-CB harmonogram w terminie 10 dni roboczych od otrzymania żądania ponownego przedłożenia. Harmonogram obejmuje planowane terminy dostarczenia zmodyfikowanego TOE i dokumentacji, a także uzgodnione z CAB-ITSEF terminy oceny. Ponowne przedłożenie następuje w terminie jednego miesiąca od otrzymania żądania ponownego przedłożenia.
- 88 Odbywa się spotkanie koordynacyjne między Wnioskodawcą, CAB-ITSEF i CAB-CB. Spotkanie to ma charakter spotkania otwierającego (patrz sekcja 7.3.1).
- 89 CAB-ITSEF ponownie bada właściwe istotne ustalenia z poprzedniej oceny.
- 90 Po zakończeniu jednorazowo rozszerzonej oceny CAB-ITSEF przedkłada zaktualizowany ETR CAB-CB. ETR zawiera nowo pozyskane ustalenia oraz ewentualnie nową opinię dotyczącą decyzji certyfikacyjnej.
- 91 Na podstawie walidacji wyników oceny CAB-CB przyjmuje zarówno wersję ze śledzeniem zmian, jak i bez niego. Dodatkowo odbywa się rozmowa końcowa.
- 92 *UWAGI:*
- 1 *Ponowne złożenie wniosku nie jest wymagane.*
 - 2 *Odpowiednie uzgodnienie umowne między Wnioskodawcą a CAB-ITSEF zawiera się z wyprzedzeniem.*
 - 3 *Jeżeli Wnioskodawca nie dotrzymuje terminów, pomimo zapytań ze strony CAB-CB, CAB-CB może zakończyć procedurę*

jednorazowo rozszerzonej oceny i zamknąć fazę procesu na podstawie pierwotnego ETR.

7.4 Faza certyfikacji

93 UWAGA: faza odzwierciedla PN-EN ISO/IEC 17065, 7.6–7.7 i 7.13.

7.4.1 Diagram

94 Zadania właściwych ról w tej podfazie przedstawiono na Rysunek 6.



Dostawca portfela EUDI	CAB-ITSEF	CAB-CB
• Możliwość wniesienia do CAB-CB pisemnego sprzeciwu wobec decyzji certyfikacyjnej (w przypadku zrzeczenia się prawa do sprzeciwu) • okres publikacji będzie krótszy • Zgoda na publikację	• Brak	• Sporządzenie decyzji certyfikacyjnej, certyfikatu oraz raportu z certyfikacji • Przekazanie decyzji certyfikacyjnej i raportu certyfikacyjnego Wnioskodawcy • Publikacja certyfikatu oraz raportu z certyfikacji

Rysunek 6 Prezentacja fazy certyfikacji

7.4.2 Opis fazy

95 Po zakończeniu końcowej oceny wyników oceny i podjęciu decyzji CAB-CB kompletuje dokumenty proceduralne i informuje Wnioskodawcę o decyzji w terminie 5 dni roboczych.

96 Jeżeli decyzja certyfikacyjna jest pozytywna, certyfikat i raport z certyfikacji zostaną przygotowane i przesłane Wnioskodawcy wraz z decyzją certyfikacyjną nie później niż w terminie 14 dni roboczych, licząc od zdarzenia opisanego w pkt 99.

97 Odwołania i skargi rozpatruje się zgodnie z postanowieniami ogólnymi zawartymi w G-01, sekcja 5.5. W każdym przypadku Wnioskodawca może złożyć oświadczenie o braku sprzeciwu, a procedura publikacji, o ile ma zastosowanie, rozpoczyna się niezwłocznie po złożeniu oświadczenia Wnioskodawcy.

- 98 Po upływie terminu na wniesienie sprzeciwu albo po jego skróceniu oświadczeniem Wnioskodawcy, oraz za zgodą Wnioskodawcy, certyfikat i raport z certyfikacji zostaną opublikowane na stronie internetowej CAB-CB.
- 99 Jeżeli decyzja certyfikacyjna jest negatywna, Wnioskodawca ma 14 dni roboczych na wniesienie do CAB-CB pisemnego sprzeciwu wobec decyzji certyfikacyjnej.
- 100 CAB-CB rozpatruje sprzeciw, o ile ma zastosowanie, w terminie 14 dni roboczych. Decyzja staje się ostateczna z upływem terminu na wniesienie sprzeciwu.

7.4.3 Dokumenty związane z certyfikacją

- 101 Raport z certyfikacji sporządzany przez CAB-CB po pozytywnym zakończeniu oceny zawiera elementy opisane w G-01, sekcja 6.3, a dodatkowo:
- krótki opis techniczny produktu,
 - wybrane informacje o wynikach oceny,
 - informacje i wymagania dotyczące zamierzonego użycia certyfikowanego produktu/komponentu w certyfikowanej konfiguracji,
 - informacje o przydatności wdrożonych mechanizmów kryptograficznych.
- 102 Raport z certyfikacji potwierdza, że ocenę przeprowadzono na podstawie uznanych procedur oraz że wymagania bezpieczeństwa określone w dokumencie Security Target — w zakresie funkcjonalności i zakresu oceny — zostały spełnione.
- 103 Wszystkie istotne informacje dotyczące korzystania z certyfikacji i znaku zgodności zamieszcza się w raporcie z certyfikacji na podstawie postanowień zawartych w sekcji 6.7.
- 104 Dokument Security Target stanowi część publikacji wyniku certyfikacji jako załącznik do raportu z certyfikacji.
- 105 Security Target może zostać przed publikacją zredagowany (sanityzowany) poprzez usunięcie lub sparafrazowanie zastrzeżonych informacji technicznych Wnioskodawcy.
- 106 W przypadku gdy Wnioskodawca zażąda sanityzacji Security Target, CAB-CB wykonuje tę czynność zgodnie z CIR (UE) 2024/482, załącznik V.2.

- 107 Certyfikat i raport z certyfikacji mogą być sporządzone w języku polskim lub angielskim. Jeżeli ETR nie jest dostępny w języku polskim, CAB-CB może zażądać od CAB-ITSEF streszczenia kluczowych punktów ETR w języku polskim.

7.5 Pracochłonność oceny i certyfikacji

- 108 Planowany nakład pracy na przeprowadzenie oceny bezpieczeństwa TOE i jego następcej certyfikacji jest następujący (patrz Tabela 5).
- 109 Wartości ujęte w Tabeli 5 są wartościami maksymalnymi i planowanymi i mogą ulec zmianie na mocy porozumienia z Właścicielem programu.

Tabela 5 Planowana pracochłonność oceny i certyfikacji

Poziom uzasadnienia zaufania	Planowana pracochłonność CAB
Pracochłonność oceny (CAB-ITSEF)	
Wysoki	— 50 dni roboczych* — Opcjonalnie: 5 dni roboczych na każdy specyficzny protokół zaimplementowany na interfejsie, w przypadku gdy Instancja Portfela integruje co najmniej jeden własnościowy protokół komunikacyjny. Walidację bezpieczeństwa tych protokołów wykonuje się dodatkowo, poza zakresem pracochłonności oszacowanym powyżej. * Obejmuje kontrole kodu źródłowego użycia WSCA (tj. pokrywa ataki związane z użyciem WSCA).
Planowana pracochłonność certyfikacji (CAB-CB)**	
Wysoki	— 14 dni roboczych ** Oszacowania nie obejmują dodatkowej pracochłonności opisanej w 7.3.4.

7.6 Postanowienia dodatkowe

- 110 Certyfikat jest ważny przez 5 lat od daty wydania.
- 111 CAB-CB powiadamia Właściciela programu o wydanym certyfikacie w terminie pięciu dni roboczych od wydania, zgodnie z procedurą ustanowioną w G-03.
- 112 CAB-ITSEF i CAB-CB archiwizują wszystkie dowody istotne odpowiednio dla oceny i certyfikacji przez okres określony w G-01, sekcja 5.9.

- 113 Wymiana informacji między CAB-CB, CAB-ITSEF i Wnioskodawcą jest zabezpieczana z użyciem najnowocześniejszych mechanizmów kryptograficznych zatwierdzonych przez Właściciela programu. Wykaz mających zastosowanie mechanizmów i aplikacji zawarto w G-03.

8 Utrzymanie certyfikatu

8.1 Postępowanie z niezgodnościami

- 114 Stosuje się postanowienia ogólne określone w G-01, sekcje 5.3 i 5.4.
- 115 Każdą podatność, niezależnie od jej krytyczności, uznaje się za niezgodność.

8.2 Ogólne podejście do zarządzania zmianą

- 116 Ogólne podejście do zarządzania zmianą dotyczącą certyfikowanego rozwiązania Portfela EUDI określono w G-01, sekcja 5.3.
- 117 W odniesieniu do programu certyfikacji GP-02, w Tabeli 6 przedstawiono role i odpowiedzialności w zarządzaniu zmianą, która wpływa na uzasadnienie zaufania wyrażone w certyfikacie certyfikowanego produktu (działania po certyfikacji).

Tabela 6 Role i odpowiedzialności w zarządzaniu zmianą

Rola	Odpowiedzialności
Posiadacz certyfikatu (wcześniej: Wnioskodawca)	— Powiadamia CAB-CB o krytycznych podatnościach / aktywnych eksploatacjach: w ciągu 24 godzin. — Powiadamia CAB-CB o podatnościach o wysokiej dotkliwości: w ciągu 3 dni. — Powiadamia CAB-CB o pozostałych zmianach/podatnościach: nie dotyczy. — Utrzymuje politykę zarządzania podatnościami zgodnie z EN ISO/IEC 30111:2019. — Przygotowuje raporty analizy wpływu (IAR) dla właściwych zmian. — Przygotowuje i wdraża poprawkę (patch) dla podatności krytycznej bez zbędnej zwłoki.
CAB-CB	— Ocenia wszystkie powiadomienia dewelopera i określa wymagane działania: w ciągu 2 dni roboczych od otrzymania powiadomienia. — Zgłasza Właścicielowi programu WSZYSTKIE incydenty i podatności, niezależnie od dotkliwości. — Kontaktuje się z CAB-ITSEF w celu zasięgnięcia opinii w kwestii technicznej IAR, jeżeli to konieczne: dodatkowe 2 dni robocze na odpowiedź CAB-ITSEF do Posiadacza certyfikatu. — Decyduje o dalszych działaniach bez zbędnej zwłoki. — Decyduje o statusie certyfikatu.

CAB-ITSEF	— Wykonuje ponowną ocenę: w ciągu maks. 4/n dni roboczych, w zależności od dotkliwości podatności, gdzie n oznacza liczbę dni pierwotnej pracochłonności oceny.
Właściciel programu	— Prowadzi centralny rejestr podatności obejmujący wszystkie certyfikowane produkty. — Analizuje wzorce w układzie między jednostkami CAB-CB i cechami produktów lub korzysta z wiarygodnych wzorców (np. baz danych utrzymywanych przez ENISA). — W razie potrzeby, wydaje wytyczne dla jednostek CAB-CB i deweloperów.

8.3 Zobowiązania posiadacza certyfikatu po certyfikacji

118 Posiadacz certyfikatu, zgodnie z GP-02, prowadzi aktywne zarządzanie podatnościami certyfikowanego produktu przez okres ważności certyfikatu. Posiadacz co najmniej:

- zapewnia punkt kontaktowy, przez który użytkownicy końcowi mogą zgłaszać podatności,
- prowadzi aktywne i stałe monitorowanie produktu pod kątem podatności (np. poprzez monitorowanie właściwych publicznie dostępnych baz danych zawierających znane podatności, ocenę i usuwanie zgłoszonych podatności),
- niezwłocznie powiadamia CAB-CB o wszelkich znanych podatnościach certyfikowanego produktu,
- zapewnia terminowe i co do zasady nieodpłatne dostarczanie odpowiednich aktualizacji usuwających lub obchodzących znane podatności, poprzez zdefiniowany kanał dystrybucji dostępny dla użytkownika końcowego (np. za pośrednictwem strony pobierania),
- powiadamia użytkowników końcowych o dostępności nowych aktualizacji bezpieczeństwa (np. poprzez biuletyn lub dziennik zmian).

8.4 Ciągłość uzasadnienia zaufania w GP-02

8.4.1 Postanowienia ogólne

119 Certyfikowany produkt podlega zmianom, niezależnie od ich źródła. Zmianą wymagającą działania może być:

- zmiana samego certyfikowanego produktu (TOE) istotna dla bezpieczeństwa,
- pojawienie się nowych podatności mogących mieć bezpośredni wpływ na certyfikowany produkt,
- zmiany środowiska, w którym działa certyfikowany produkt.

120 Ilekroć zmiana jest istotna dla bezpieczeństwa, podejmuje się odpowiednie działanie w odniesieniu do ciągłości uzasadnienia zaufania.

8.4.2 Ponowna ocena i ponowna certyfikacja

121 Do ponownej oceny lub ponownej certyfikacji TOE wymagany jest opis zmian w raporcie analizy wpływu (IAR). Wszelkie zmiany istotne dla bezpieczeństwa określa się w IAR.

122 Posiadacz certyfikatu przygotowuje opis zmian wraz z raportem analizy wpływu (IAR) do wniosku o certyfikację. Na tej podstawie CAB-CB, z udziałem CAB-ITSEF, decyduje o wymaganej zmianie (redukcji) pracochłonności oceny.

123 Zakres oceny ustala się między CAB-CB a CAB-ITSEF na spotkaniu otwierającym; na podstawie zmiany cech produktu określonej w IAR oraz dowodów Posiadacza certyfikatu jednostki CAB oceniają, które kroki oceny należy powtórzyć, a które wcześniejsze wyniki oceny można wykorzystać ponownie.

124 Specyfikacja ta jest wymagana, aby umożliwić ponowne wykorzystanie wcześniejszych wyników oceny, a następnie umożliwić planowanie przyrostowe (delta) przez CAB-ITSEF.

125 Regulacje te stosuje się analogicznie do ponownej oceny, jeżeli wcześniej przeprowadzono pełną ocenę z wynikiem negatywnym.

126 Po pozytywnym zakończeniu oceny wyniki techniczne są dokumentowane przez CAB-CB w zaktualizowanym raporcie z certyfikacji, a w zależności od tych wyników wydawany jest:

- dotychczasowy certyfikat ze zmienionym zakresem, bez zmiany okresu ważności, albo
- dotychczasowy certyfikat z wydłużonym okresem ważności, albo
- nowy certyfikat.

- 127 W przypadku podatności krytycznej Posiadacz certyfikatu przygotowuje i wdraża odpowiednią poprawkę bezpieczeństwa bez zbędnej zwłoki. Dalsze działania obejmują wszystkie pozostałe kroki opisane w niniejszej sekcji.

8.4.3 Zawieszenie lub cofnięcie certyfikatu

- 128 CAB-CB zawiesza certyfikat, gdy dalsza zgodność budzi wątpliwości. Okres zawieszenia nie przekracza 42 dni. Każde przedłużenie wymaga decyzji Właściciela programu, ale w żadnym przypadku nie może przekroczyć stu dni.
- 129 Okres zawieszenia nie ma wpływu na okres ważności certyfikatu.
- 130 Posiadacz certyfikatu powiadamia użytkowników rozwiązania Portfela EUDI oraz właściwych interesariuszy ekosystemu Portfela EUDI o zawieszeniu i o podanych przez CAB-CB powodach zawieszenia, z wyjątkiem tych części uzasadnienia, których udostępnienie stanowiłoby ryzyko bezpieczeństwa lub które zawierają informacje wrażliwe.
- 131 CAB-CB cofa certyfikat, gdy niezgodność ma charakter trwały lub nie została usunięta w wymaganym terminie, albo gdy Posiadacz certyfikatu zaprzestaje utrzymywania certyfikowanego produktu.
- 132 CAB-CB powiadamia Właściciela programu o cofnięciu certyfikatu. Jednostka certyfikująca powiadamia organ nadzoru rynku oraz krajową jednostkę akredytującą.
- 133 Posiadacz certyfikatu może wnioskować o cofnięcie certyfikatu.

8.5 Nadzór

8.5.1 Coroczne działania w nadzorze

- 134 Nadzór obejmuje działania inne niż działania związane z ciągłością uzasadnienia zaufania (patrz sekcja 8.4).
- 135 Działania w nadzorze prowadzi CAB-CB z udziałem CAB-ITSEF.
- 136 Plan działań w nadzorze przedstawiono w Tabeli 7.

Tabela 7 Działania w nadzorze w okresie ważności certyfikatu

Rok	Rodzaj działania	Działania obowiązkowe
1	Nadzór	— Ocena skuteczności działania procesów utrzymania (zarządzanie zmianą, dostarczanie aktualizacji, zarządzanie podatnościami)*. — Ocena zmian w Instancji Portfela od ostatniej oceny / ponownej oceny, w tym ponowne sprawdzenie użycia WSCA dla każdego zmienionego kodu. — Weryfikacja, że certyfikaty WSCA i WSCD pozostają ważne i obejmują zakres odpowiedni do użycia.
2	Nadzór	— Zaktualizowana ocena podatności Instancji Portfela. — Ocena skuteczności działania procesów utrzymania*. — Ocena zmian od ostatniej oceny.
3	Nadzór	— Ocena skuteczności działania procesów utrzymania*. — Ocena zmian od ostatniej oceny.
4	Ponowna certyfikacja	— Pełna ponowna ocena. — Ocena uproszczona z uwzględnieniem komponentów niezmienionych, z uzasadnieniem CAB-CB. — Zaktualizowana ocena podatności. — Ocena skuteczności działania procesów utrzymania. — Nowy certyfikat zgodności.
<i>* Wyniki działań w nadzorze z GP-03 mogą być wykorzystane ponownie.</i>		

137 Wszystkie działania w nadzorze kończą się w ciągu 12 miesięcy od oceny przeprowadzonej w roku poprzednim.

8.5.2 Wynik nadzoru

138 Po każdym nadzorze CAB-CB przeprowadza przegląd i podejmuje decyzję certyfikacyjną o jednym z następujących możliwych rozstrzygnięć:

- kontynuacja certyfikatu, bez jakichkolwiek zmian,

- zawieszenie certyfikatu wraz z wymaganiami wobec Posiadacza certyfikatu dotyczącymi usunięcia zidentyfikowanych niezgodności w określonym terminie; Posiadacz certyfikatu jest zobowiązany przygotować IAR i stosuje się procedurę zarządzania zmianą (patrz sekcja 8.4),
- cofnięcie certyfikatu w przypadku niezgodności, których nie można usunąć; Posiadacz certyfikatu jest zobowiązany przygotować IAR i stosuje się procedurę zarządzania zmianą (patrz sekcja 8.4).

8.6 Skutki zmian certyfikatów GP-01 / GP-03

139 W przypadku zawieszenia certyfikatu (certyfikatów) GP-01 lub GP-03 jednostka CAB-CB działająca w ramach GP-02:

- I. inicjuje ocenę wpływu w celu ustalenia, czy zawieszenie wpływa na zgodność certyfikowanego rozwiązania Portfela EUDI z wymaganiami WP-02;
- II. jeżeli ocena wpływu wykaże, że zgodność jest istotnie naruszona — zawiesza certyfikat GP-02 do czasu rozstrzygnięcia;
- III. jeżeli ocena wpływu wykaże, że zgodność nie jest istotnie naruszona — dokumentuje uzasadnienie i kontynuuje nadzór.

9 Postanowienia końcowe

9.1 Ustawodawstwo krajowe

- 140 Program certyfikacji cyberbezpieczeństwa GP-02 ustanawia się zgodnie z właściwym polskim aktem prawnym.

9.2 Umowy o ocenę i certyfikację

- 141 CAB-ITSEF może zawrzeć odrębną umowę z Wnioskodawcą albo działać jako podwykonawca CAB-CB.
- 142 W przypadku odrębnej umowy nie może ona zawierać postanowień, które utrudniałyby prawidłową ocenę, a w szczególności takich, które mogłyby utrudniać przekazywanie CAB-CB informacji o ustaleniach wynikających z oceny.
- 143 Umowa o ocenę uwzględnia, że podczas spotkania otwierającego lub w toku procedury mogą pojawić się nowe lub dodatkowe kwestie mogące wpłynąć na proces oceny (patrz sekcja 7.3.4), stosownie do uznania CAB-CB.
- 144 CAB-CB zawiera umowę z Wnioskodawcą na podstawie postanowień GP-02.
- 145 Uzgodnienia umowne mogą być narzucone przez Właściciela programu.

9.3 Koszty

- 146 Wszystkie koszty ustala się na podstawie rzeczywistej pracochłonności oceny i certyfikacji.
- 147 Do GP-02 stosuje się ogólne zasady określania wszelkich kosztów i wydatków określone w G-01.

Załączniki

148 Następujące informacje stanowią część GP-02 (patrz Tabela 8). Te załączniki pozostają w angielskiej wersji językowej.

Tabela 8 Wykaz załączników

Załącznik	Tytuł
Załącznik A	Szablon Security Target dla Instancji Portfela
Załącznik B	Wymagania dotyczące oceny bezpiecznego przewodnika użytkownika (Secure User Guide)
Załącznik C	Wymagania dotyczące oceny specyfikacji funkcjonalnej i projektu TOE
Załącznik D	Wymagania dotyczące oceny mechanizmów kryptograficznych