

GP-03

System Certyfikacji PL Portfela EUDI

Program Certyfikacji eID

WERSJA 1.01

2026.07.09

Oznaczenie dokumentu	GP-03
Wersja	V1.01 (2026-07)
Status	FINALNA
Data	09.07.2026
Rodzaj dokumentu	Program certyfikacji — specyfikacja programu (PN-EN ISO/IEC 17067)
Ramy nadrzędne	G-01, G-02, G-03, G-04, G-05
Właściciel programu	Rzeczpospolita Polska / Minister Cyfryzacji
Przedmiot certyfikacji	System identyfikacji elektronicznej i usługi z nim związane
Odbiorcy pierwotni	Jednostki oceniające zgodność (CAB)
Odbiorcy wtórni	Dostawca EUDI, dostawca PID
Poziom uzasadnienia zaufania <potwierdzanie tożsamości>	Wysoki (CIR (UE) 2015/1502)
Dokumenty podrzędne	Serie WZ-03, WP-03, WZ-03

Historia zmian

Lp.	Zmiana	Wersja	Data
1.	Wersja oficjalna	1.0	2026-06-09
2.	Punkt 7.8 „Ustalanie zakresu polegania” przeniesiony do G-01; Załącznik B „Ramy audytu” przeniesiony z WM-03-00; dodano rozdział 9 z procedurami wydawania i nadzoru nad certyfikatem najwyższego poziomu; zmiany redakcyjne	1.01	2026-07-09

Spis treści

1	PRZEDMOWA	8
2	ZAKRES.....	9
3	PODSTAWA PRAWNA.....	10
4	ODNIESIENIA	12
4.1	Normy i specyfikacje techniczne	12
4.2	Dokumenty nadrzędne	12
4.3	Dokumenty równorzędne	12
4.4	Dokumenty podrzędne	12
5	TERMINY I DEFINICJE.....	13
6	STRUKTURA PROGRAMU CERTYFIKACJI	14
6.1	Przedmioty certyfikacji.....	14
6.2	Role i obowiązki	15
6.2.1	Przegląd interesariuszy programu	15
6.2.2	Akredytacja jednostek CAB	15
6.3	Mechanizmy zapewnienia bezstronności.....	16
6.4	Relacja do GP-01 i GP-02	16
6.5	Relacja do dokumentów podrzędnych WZ-03, WP-03 i WM-03.....	17
6.6	Typ programu	17
6.7	Wykorzystanie certyfikacji i znaków zgodności.....	17
7	RAMY OCENY	19
7.1	Postanowienia ogólne	19
7.2	Zakres oceny	19
7.3	Metody oceny	20
7.4	Rodzaje dowodów	21
7.5	Proporcjonalność.....	22
7.6	Akceptowalność i ponowne wykorzystanie dowodów uzasadnienia zaufania	22
7.7	Kryteria oceny.....	23
8	PROCES CERTYFIKACJI	25
8.1	Postanowienia ogólne	25
8.2	Faza przygotowania i wniosku	25
8.3	Faza oceny	26
8.3.1	Spotkanie otwierające.....	26
8.3.2	Ocena	26

8.4	Faza certyfikacji	26
8.5	Nakłady na ocenę i certyfikację	27
8.6	Postanowienia dodatkowe	27
8.7	Certyfikat zgodności	27
8.8	Nadzór	28
8.9	Recertyfikacja	30
8.10	Zawieszenie i cofnięcie	31
8.11	Skutki zmian certyfikatów GP-01 / GP-02	32
9	DZIAŁANIA ZWIĄZANE Z CERTYFIKATEM NAJWYŻSZEGO POZIOMU	33
9.1	Wydanie certyfikatu najwyższego poziomu	33
9.2	Nadzór	33
9.3	Zmiany przedmiotu certyfikacji najwyższego poziomu	34
9.4	Zawieszenie, zakończenie i cofnięcie certyfikatu	34
10	POSTANOWIENIA KOŃCOWE	35
10.1	Ustawodawstwo krajowe	35
10.2	Umowy certyfikacyjne	35
10.3	Koszty	35
	ZAŁĄCZNIK A (NORMATYWNY) — PRZYPISANIE WYMAGAŃ DO DOKUMENTÓW PODRZĘDNYCH	36
A.1	WYMAGANIA Z ROZPORZĄDZENIA (UE) NR 910/2014 (EIDAS)	36
A.2	WYMAGANIA Z CIR (UE) 2015/1502	36
A.3	WYMAGANIA Z CIR (UE) 2024/2977	37
A.4	WYMAGANIA Z CIR (UE) 2024/2979	37
A.5	WYMAGANIA Z CIR (UE) 2024/2981	37
A.6	WYMAGANIA Z CIR (UE) 2024/2690	38
	ZAŁĄCZNIK B RAMY AUDYTU	39
B.1	CEL	39
B.2	ZAKRES	39
B.3	ODNIESIENIA, TERMINY I ROLE	40
B.3.1	Odniesienia	40
B.3.2	Role i odpowiedzialności	40
B.3.3	Terminy specyficzne dla ram audytu cyberbezpieczeństwa	41
B.4	OGÓLNE ZASADY AUDYTU	41
B.5	CELE, ZAKRES I CZAS AUDYTU	42

B.5.1 Cele audytu	42
B.5.2 Zakres audytu	42
B.5.3 Czas audytu	43
B.6 PLANOWANIE AUDYTU I SPOTKANIE OTWIERAJĄCE	44
B.7 METODY I TECHNIKI AUDYTU	45
B.7.1 Przegląd dokumentacji	45
B.7.2 Wywiady	45
B.7.3 Obserwacja i inspekcja	45
B.7.4 Analiza zapisów, logów i transakcji.....	46
B.7.5 Testowanie i weryfikacja techniczna.....	46
B.7.6 Techniki audytu zdalnego.....	46
B.8 DOWODY AUDYTOWE I PRÓBKOWANIE	46
B.8.1 Wystarczalność i odpowiedniość	46
B.8.2 Próbkowanie.....	47
B.8.3 Wiele lokalizacji	47
B.9 ZEWNĘTRZNY MATERIAŁ DOWODOWY UZASADNIENIA ZAUFANIA.....	48
B.9.1 Ocena akceptowalności	48
B.9.2 Wykorzystanie zewnętrznego materiału dowodowego uzasadnienia zaufania w planowaniu i realizacji audytu.....	48
B.10 KOMPETENCJE, NIEZALEŻNOŚĆ I OUTSOURCING ZESPOŁU AUDYTOWEGO	49
B.10.1 Kompetencje zbiorowe.....	49
B.10.2 Kierownik zespołu audytowego i eksperci techniczni	49
B.10.3 Outsourcing czynności audytowych.....	50
B.11 PROCES AUDYTU	50
B.11.1 Audyty początkowe i audyty ponownej oceny	50
B.11.2 Etap 1 — przegląd dokumentacji i gotowości.....	50
B.11.3 Etap 2 — wdrożenie i skuteczność operacyjna.....	51
B.11.4 Audyty nadzoru i audyty specjalne	51
B.11.5 Spotkania i komunikacja.....	51
B.12 OCENA USTALEŃ I ZASADY ZALICZENIA/NIEZALICZENIA.....	52
B.12.1 Zastosowanie wymagań	52
B.12.2 Wyniki oceny na poziomie wymagań	52
B.12.3 Spostrzeżenia	53
B.12.4 Związek z decyzją certyfikacyjną.....	53
B.13 RAPORTOWANIE Z AUDYTU I POWIĄZANIE Z RAPORTEM Z OCENY	53

B.13.1 Raport z audytu	53
B.13.2 Raport z oceny	54
B.14 DZIAŁANIA KORYGUJĄCE I DZIAŁANIA NASTĘPCZE	54
B.15 NADZÓR, PONOWNA OCENA I AUDYTY SPECJALNE	55
B.16 ZAPISY, POUFNOŚĆ I KONTROLA JAKOŚCI	55
ANEKS C (NORMATYWNY) MINIMALNA ZAWARTOŚĆ PLANU AUDYTU	57
ANEKS D (NORMATYWNY) MINIMALNA ZAWARTOŚĆ ZAPISU DOWODOWEGO Z AUDYTU	58
ANEKS E (NORMATYWNY) MATRYCA WYNIKÓW OCENY	59

1 **Przedmowa**

- 1 W niniejszym dokumencie (GP-03) przedstawiono specyfikację Programu Certyfikacji eID — jednego z trzech programów certyfikacji w ramach Systemu Certyfikacji PL Portfela EUDI ustanowionego przez Rzeczpospolitą Polską. Definiuje on program certyfikacji — w rozumieniu PN-EN ISO/IEC 17067 — który akredytowane jednostki certyfikujące (CAB) stosują przy certyfikacji systemu identyfikacji elektronicznej, w ramach którego dostarczany jest Europejski Portfel Tożsamości Cyfrowej.
- 2 GP-03 jest adresowany przede wszystkim do CAB prowadzących działania certyfikacyjne w ramach Programu Certyfikacji eID. Dostawcy usług podlegający certyfikacji (dostawca EUDI i dostawca PID) powinni czytać niniejszy dokument łącznie z mającymi zastosowanie dokumentami podrzędnymi WZ-03 i WP-03, które określają wymagania merytoryczne, jakie mają spełniać.
- 3 Niniejszy dokument stanowi część serii GP, funkcjonującej w ramach ładu ustanowionego przez serię G (ramy programowe). Powinien być czytany łącznie z G-01 (System Certyfikacji PL Portfela EUDI) oraz G-03 (Organizacja i wsparcie właściciela krajowego programu certyfikacji EUDI).

2 Zakres

- 4 W dokumencie określono program certyfikacji systemu identyfikacji elektronicznej, w ramach którego Rzeczpospolita Polska dostarcza Europejski Portfel Tożsamości Cyfrowej, w ramach Systemu Certyfikacji PL Portfela EUDI.
- 5 Przedmiot certyfikacji w ramach GP-03 obejmuje usługi polegające na dostarczaniu i eksploatacji rozwiązań portfela oraz systemów identyfikacji elektronicznej, w ramach których są one dostarczane.
- 6 GP-03 ustanawia wymagania dotyczące usług (poprzez odesłanie do dokumentów podrzędnych), metodykę oceny (poprzez odesłanie do załącznika B oraz do dokumentów podrzędnych) oraz procedury oceny zgodności, które akredytowane jednostki CAB stosują przy certyfikacji systemu eID i dostawców usług działających w jego ramach. Dokument należy czytać łącznie z G-05, który określa wymagania akredytacyjne wobec samych jednostek certyfikujących.
- 7 W kontekście niniejszego programu certyfikacji przedmiotem certyfikacji jest system identyfikacji elektronicznej, obejmujący rozwiązania organizacyjne i procesy dostawcy portfela oraz dostawcy PID, które łącznie zapewniają osobom fizycznym usługi związane z portfelem. Certyfikacja obejmuje zgodność systemu eID i jego dostawców usług z wymaganiami ustanowionymi w dokumentach podrzędnych WZ-03, WP-03 i WM-03.

3 Podstawa prawna

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

- I. Rozporządzenie (UE) 910/2014, w szczególności art. 5a i 5c;
- II. 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;
- III. Rozporządzenie wykonawcze Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. w sprawie integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej;
- IV. Rozporządzenie wykonawcze Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie danych identyfikujących osobę wydawanych do europejskich portfeli tożsamości cyfrowej;
- V. Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie poziomów uzasadnienia zaufania środków identyfikacji elektronicznej — załącznik, pkt 2.4;
- VI. Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. w sprawie środków zarządzania ryzykiem w cyberbezpieczeństwie;
- VII. Rozporządzenie wykonawcze Komisji (UE) 2026/798 z dnia 7 kwietnia 2026 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących zdalnego onboardingu użytkowników do europejskich portfeli tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej o poziomie uzasadnienia zaufania „średnim” w połączeniu z dodatkowymi procedurami zdalnego onboardingu, w przypadku gdy takie połączenie spełnia wymagania poziomu uzasadnienia zaufania „wysokiego”;
- VIII. Rozporządzenie (UE) 765/2008 w sprawie akredytacji i nadzoru rynku, w szczególności art. 4 i 5;
- IX. Ustawa z dnia 24 września 2010 r. o ewidencji ludności.
- X. Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych
- XI. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 lutego 2019 r. w sprawie warstwy elektronicznej dowodu osobistego

- XII. Rozporządzenie Ministra Cyfryzacji z dnia 15 października 2021 r. w sprawie prowadzenia Rejestru Dowodów Osobistych
- XIII. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.
- XIV. Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel.
- XV. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4 Odniesienia

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

4.2 Dokumenty nadrzędne

- 11 G-01. System Certyfikacji PL Portfela EUDI
- 12 G-02. Słownik
- 13 G-03. Organizacja i wsparcie właściciela krajowego Programu Certyfikacji EUDI
- 14 G-04. Opracowywanie i utrzymywanie rejestru ryzyk związanych z wdrożeniem i certyfikacją portfela EUDI Wallet
- 15 G-05. Wymagania akredytacyjne dla jednostek CAB

4.3 Dokumenty równorzędne

- 16 GP-01. Program Certyfikacji Funkcjonalnej EUDI Wallet
- 17 GP-02. Program Certyfikacji Cyberbezpieczeństwa EUDI Wallet

4.4 Dokumenty podrzędne

- 18 WZ-03-01. Wymagania organizacyjne i techniczne dla dostawców eID
- 19 WZ-03-02. Wymagania organizacyjne i techniczne dla dostawców PID, w tym wymagania określone w art. 5c rozporządzenia (UE) 910/2014
- 20 WZ-03-03. Wymagania organizacyjne i techniczne dla dostawców Portfela EUDI (dawniej oznaczone jako WZ-01)
- 21 WP-03-01. Wymagania dotyczące rejestracji PID oraz cyklu życia PID/Portfela EUDI
- 22 WP-03-02. Wymagania dotyczące rejestracji Portfela EUDI
- 23 WP-03-03. Wymagania dotyczące eID (w tym uwierzytelniania)
- 24 WM-03-01. Ramy audytu cyberbezpieczeństwa dla dostawców PID
- 25 WM-03-02. Ramy audytu cyberbezpieczeństwa dla dostawców eID
- 26 WM-03-03. Ramy audytu cyberbezpieczeństwa dla dostawców Portfela EUDI

5 Terminy i definicje

27 Na potrzeby niniejszego dokumentu wszystkie terminy i definicje zawarte są w dokumencie G-02. Słownik.

6 Struktura programu certyfikacji

6.1 Przedmioty certyfikacji

- 28 Przedmiotem certyfikacji w ramach niniejszego programu jest system identyfikacji elektronicznej, w ramach którego dostarczane są europejskie portfele tożsamości cyfrowej, o których mowa w art. 5c ust. 1 rozporządzenia (UE) 910/2014. Certyfikacja obejmuje zarówno rozwiązania w zakresie ładu na poziomie systemu, jak i usługi operacyjne świadczone przez dostawcę Portfela EUDI oraz dostawcę PID.
- 29 CAB ocenia zgodność przedmiotu certyfikacji z zestawem wymagań ustanowionych w dokumentach podrzędnych WZ-03, WP-03 i WM-03, zgodnie z przypisaniem w Tabeli 1 poniżej.
- 30 *UWAGA: W kontekście programu certyfikacji GP-03 za CAB uznaje się wyłącznie jednostkę certyfikującą.*

Tabela 1 Przypisanie dokumentów z wymaganiami do ról

Dokument	Tytuł	Ma zastosowanie do
WZ-03-01	Wymagania organizacyjne i techniczne dla dostawców eID	dostawca PID, dostawca portfela
WZ-03-02	Wymagania organizacyjne i techniczne dla dostawców PID (w tym art. 5c eIDAS)	dostawca PID
WZ-03-03	Wymagania organizacyjne i techniczne dla dostawców Portfela EUDI (w tym art. 5c eIDAS)	dostawca portfela
WP-03-01	Rejestracja PID oraz cykl życia PID/Portfela EUDI	dostawca PID
WP-03-02	Wymagania dotyczące rejestracji Portfela EUDI	dostawca portfela
WP-03-03	Wymagania dotyczące środków eID (w tym uwierzytelniania)	dostawca PID
WM-03-01	Ramy audytu cyberbezpieczeństwa — dostawcy PID	CAB
WM-03-02	Ramy audytu cyberbezpieczeństwa — dostawcy eID	CAB
WM-03-03	Ramy audytu cyberbezpieczeństwa — rejestracja PID i cykl życia	CAB

- 31 *UWAGA — W przypadku gdy role dostawcy portfela i dostawcy PID pełni ten sam podmiot prawny, CAB ocenia ten podmiot zarówno według wymagań WZ-03-03 i WZ-03-02, jak i według WP-03-01 i WP-03-02.*

6.2 Role i obowiązki

6.2.1 Przegląd interesariuszy programu

32 Przegląd ról i obowiązków przedstawiono w Tabeli 2.

Tabela 2 Przegląd ról i obowiązków

Rola	Obowiązki	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	Planuje, przeprowadza i dokumentuje ocenę; podejmuje decyzję certyfikacyjną i wydaje certyfikat zgodności; zarządza działaniami nadzorczymi i recertyfikacyjnymi.	PN-EN ISO/IEC 17065; G-05
Wnioskodawca / posiadacz certyfikatu	Zgłasza system eID do certyfikacji; dostarcza dowody na potrzeby oceny; wypełnia obowiązki po certyfikacji, w tym współpracę w ramach nadzoru i notyfikację zmian. W przypadku gdy ten sam podmiot działa zarówno jako dostawca portfela, jak i dostawca PID, podlega wymaganiom WZ-03-01, WZ-03-02, WZ-03-03 oraz mających zastosowanie dokumentów WP-03.	GP-03
Krajowa jednostka akredytująca (NAB)	Akredytuje jednostki CAB zgodnie z PN-EN ISO/IEC 17065 w odpowiednim zakresie w ramach niniejszego programu.	rozporządzenie (WE) nr 765/2008
Organy nadzoru rynku	Nadzór nad certyfikowanymi usługami na rynku. Rolę tę pełnić będzie właściciel programu.	PN-EN ISO/IEC 17067; GP-03

6.2.2 Akredytacja jednostek CAB

33 CAB działające w ramach niniejszego programu muszą być akredytowane przez krajową jednostkę akredytującą zgodnie z PN-EN ISO/IEC 17065 w zakresie obejmującym GP-03 i dokumenty podrzędne. Wymagane kompetencje oraz pozostałe wymagania akredytacyjne określa G-05.

34 Ogólne postanowienia dotyczące akredytacji CAB, w tym wymagania co do zakresu akredytacji oraz uznawania akredytacji udzielonej przez inne krajowe jednostki akredytujące w UE, zawarte są w G-05 i G-01.

6.3 Mechanizmy zapewnienia bezstronności

- 35 CAB jest zobowiązana do wdrożenia mechanizmów zapewnienia bezstronności zgodnie z PN-EN ISO/IEC 17065. Bezstronność jednostki CAB gwarantują następujące mechanizmy:
- I. deklaracje bezstronności składane przez certyfikatorów przed rozpoczęciem procesu;
 - II. regularne, wyrywkowe audyty proceduralne prowadzone przez właściciela programu;
 - III. systemy zarządzania jakością stosowane do badania potencjalnych przesłanek stronniczości i wywierania wpływu.
- 36 Ogólne postanowienia dotyczące wymagań w zakresie bezstronności zawarte są w G-05.

6.4 Relacja do GP-01 i GP-02

- 37 GP-03 jest jednym z trzech programów certyfikacji w ramach Systemu Certyfikacji PL Portfela EUDI (G-01). GP-01 (Program Certyfikacji Funkcjonalnej Portfela EUDI) dotyczy zgodności funkcjonalnej aplikacji portfela; GP-02 (Program Certyfikacji Cyberbezpieczeństwa Portfela EUDI) dotyczy certyfikacji cyberbezpieczeństwa rozwiązania portfela — w obu przypadkach traktowanych jako wyrób. Te programy certyfikacji definiują wymagania oceniane i certyfikowane niezależnie od GP-03, jednak wynikające z nich certyfikaty stanowią warunek konieczny certyfikacji w ramach GP-03.
- 38 CAB oceniająca dostawcę PID według WZ-03-01 i WZ-03-02 oraz dostawcę Portfela EUDI według WZ-03-03, w ramach oceny weryfikuje, czy dostawca Portfela EUDI posiada ważne certyfikaty GP-01 i GP-02 obejmujące wersję (wersje) rozwiązania portfela objęte zakresem oceny GP-03. Program dopuszcza składanie przez dostawcę portfela deklaracji, że odpowiednie procesy oceny i certyfikacji w ramach GP-01 lub GP-02, albo obu tych programów, są w toku. Wymaganie powyższe obejmuje też certyfikat lub deklarację zgodności odnośnie do usług dostawcy PID. CAB ocenia zakres i aktualność tych certyfikatów lub deklaracji, nie jest jednak zobowiązana do ponownej oceny wymagań już nimi objętych.
- 39 W przypadku zawieszenia, cofnięcia lub wygaśnięcia certyfikatu GP-01 lub GP-02 lub certyfikatu pod GP-03 dla usług dostawcy PID, dostawca Portfela EUDI bez zbędnej zwłoki powiadamia właściciela programu oraz swoją

jednostkę oceny zgodności (CAB) dla GP-03. Skutki dla certyfikatów GP-03 opisano w pkt 8.11.

6.5 Relacja do dokumentów podrzędnych WZ-03, WP-03 i WM-03

40 Dokumenty podrzędne GP-03 — WZ-03-01 do WZ-03-03, WP-03-01 do WP-03-03 oraz WM-03-01 do WM-03-03 — stanowią normatywną treść Programu Certyfikacji eID. Określają one odpowiednio:

- I. WZ-03-0x (wymagania dotyczące systemu zarządzania) — wymagania organizacyjne, dotyczące ładu i bezpieczeństwa informacji mające zastosowanie do każdej kategorii dostawcy usług, w tym dostawcy portfela (WZ-03-01). Są one spójne z wymaganiami PN-EN ISO/IEC 27001.
- II. WP-03-0x (wymagania dotyczące usług i procesów) — wymagania procesowe dla kluczowych procesów operacyjnych systemu eID: rejestracji PID i cyklu życia, rejestracji jednostki portfela oraz zarządzania środkami eID.
- III. WM-03-0x (metody i techniki oceny) — ramy audytu cyberbezpieczeństwa, które jednostki CAB stosują przy ocenie zgodności z wymaganiami WZ-03 i WP-03. Adresowane są przede wszystkim do CAB.

41 ***UWAGA — Załącznik A do niniejszego dokumentu zawiera normatywne przypisanie wymagań prawnych do dokumentów podrzędnych. Przypisanie to potwierdza, który dokument podrzędny realizuje poszczególne wymagania prawne wynikające z właściwych aktów UE.***

6.6 Typ programu

42 Niniejszy program certyfikacji jest zgodny z modelem typu 6 zdefiniowanym w PN-EN ISO/IEC 17067, obejmującym badania i ocenę początkową, nadzór nad świadczeniem usługi oraz okresową ponowną ocenę. Program określa elementy wymienione w pkt 6.5 normy PN-EN ISO/IEC 17067, zgodnie z art. 4 ust. 3 lit. a) rozporządzeniem wykonawczym Komisji (UE) 2024/2981.

6.7 Wykorzystanie certyfikacji i znaków zgodności

43 Jako znak zgodności dla certyfikacji wydawanych w ramach niniejszego programu stosuje się wyłącznie Znak PL Portfela EUDI zdefiniowany w G-

03. W ramach programu certyfikacji GP-03 nie definiuje się żadnych dodatkowych znaków zgodności. Wyjątek stanowi certyfikat najwyższego poziomu, który może być opatrzony także europejskim znakiem zgodności, zgodnie z zasadami wskazanymi w dokumencie G-03.

44 Wspólne wymagania dotyczące wykorzystania certyfikacji i znaków zgodności określone są w G-01 i G-03.

45 CAB odpowiada za przyznawanie, zawieszanie i cofanie prawa do posługiwania się znakiem zgodności stosownie do podejmowanych przez siebie decyzji certyfikacyjnych w ramach niniejszego programu. W przypadku zawieszenia lub cofnięcia certyfikatu, odpowiednio dostawca Portfela EUDI lub dostawca PID bez zbędnej zwłoki zaprzestaje posługiwania się znakiem zgodności.

7 Ramy oceny

7.1 Postanowienia ogólne

46 W niniejszym rozdziale określono ogólną metodykę oceny, którą jednostki CAB stosują przy ocenie zgodności systemu identyfikacji elektronicznej i usług z nim związanych z wymaganiami określonymi w dokumentach podrzędnych WZ-03, WP-03 i WM-03.

47 Działania oceniające prowadzone są zgodnie z wymaganiami procesowymi określonymi w G-05 (rozdział 7) oraz planowane, realizowane i dokumentowane zgodnie z procedurami ustanowionymi przez CAB. Działania oceniające uwzględniają minimalne wymagania dotyczące oceny systemu identyfikacji elektronicznej określone w załączniku VI do rozporządzenia wykonawczego Komisji (UE) 2024/2981, w tym ocenę rejestru ryzyka. Rejestr ryzyka właściwy dla Programu Certyfikacji PL Portfela EUDI tworzy dostawca portfela na podstawie szablonu udostępnionego w G-04.

7.2 Zakres oceny

48 Zakres oceny obejmuje system identyfikacji elektronicznej (eID) oraz usługi związane z dostarczaniem i eksploatacją rozwiązania Portfela EUDI. Ocena obejmuje co najmniej:

- I. zarządzanie organizacyjne i zarządzanie bezpieczeństwem informacji dostawcy eID, zgodnie z WZ-03-01;
- II. zarządzanie organizacyjne i zarządzanie bezpieczeństwem informacji dostawcy PID, zgodnie z WZ-03-02;
- III. wymagania organizacyjne i techniczne mające zastosowanie do dostawcy portfela, zgodnie z WZ-03-03;
- IV. procesy rejestracji PID i zarządzania cyklem życia, zgodnie z WP-03-01;
- V. proces rejestracji jednostki portfela, zgodnie z WP-03-02;
- VI. wymagania dotyczące systemu eID, zgodnie z WP-03-03;
- VII. rejestr ryzyka i związane z nim postępowanie z ryzykiem wraz z zabezpieczeniami wdrożonymi w rozwiązaniu portfela.

49 W przypadku gdy system opiera się na usługach świadczonych przez strony trzecie (usługi zlecane na zewnątrz lub podwykonawstwo), zakres

oceny rozciąga się na te usługi w takim stopniu, w jakim są one istotne dla spełnienia wymagań certyfikacyjnych, zgodnie z WZ-03-03.

- 50 W przypadku gdy dostępne są zewnętrzne dowody uzasadnienia zaufania, ocenione jako akceptowalne zgodnie z pkt 7.6 CAB może ograniczyć zakres własnych działań oceniających w odniesieniu do wymagań objętych tymi dowodami. Zakres certyfikacji nie podlega ograniczeniu na podstawie zewnętrznych dowodów uzasadnienia zaufania.

7.3 Metody oceny

- 51 CAB stosuje jedną lub więcej z poniższych metod oceny, odpowiednio do charakteru ocenianego wymagania i zgodnie z dalszymi postanowieniami mających zastosowanie ram audytu WM-03.

- I. przegląd dokumentacji — badanie polityk, procedur, zapisów, umów, ocen ryzyka i innych udokumentowanych informacji utrzymywanych przez dostawcę PID, Ministerstwo Cyfryzacji lub ich dostawców usług;
- II. wywiad — ustrukturyzowane rozmowy z właściwym personelem dostawcy PID lub Właściciela programu w celu weryfikacji zrozumienia, wdrożenia i skuteczności operacyjnej wymagań;
- III. obserwacja — bezpośrednia obserwacja procesów, systemów, obiektów i praktyk operacyjnych w siedzibie dostawcy PID w Warszawie oraz w innych właściwych lokalizacjach;
- IV. badania techniczne – badanie zabezpieczeń technicznych, w tym ocena podatności, przegląd konfiguracji i testy bezpieczeństwa, odpowiednio do natury oraz poziomu ryzyka w systemie poddanym ocenie, jak określono w mającym zastosowanie dokumencie WM-03;
- V. próbkowanie — w przypadku gdy pełna ocena wszystkich wystąpień procesu powtarzalnego jest niewykonalna, CAB może zastosować próbkowanie zgodnie z wymaganiami dotyczącymi uzasadnienia zaufania określonymi w załączniku B. Metodyka próbkowania jest dokumentowana w planie oceny.

- 52 CAB określa odpowiednią kombinację metod oceny dla każdego działania oceniającego, uwzględniając charakter wymagania, poziom ryzyka, dojrzałość systemów zarządzania dostawcy PID i dostawcy portfela oraz wytyczne zawarte w mających zastosowanie ramach audytu WM-03.

7.4 Rodzaje dowodów

- 53 CAB uzyskuje wystarczające i odpowiednie dowody na poparcie swoich wniosków z oceny. Dowody mogą obejmować między innymi udokumentowane polityki, procedury i zapisy utrzymywane przez dostawcę PID i dostawcę portfela;
- I. konfiguracje systemów i dokumentację techniczną całego wyrobu lub usługi dostarczanej przez dostawcę portfela, obejmującą zarówno komponenty instancji portfela działające na urządzeniu użytkownika, jak i komponenty serwerowe (back-end) zarządzane przez dostawcę portfela, w tym usługi wydawania poświadczeń jednostki portfela (WUA), zarządzanie kontami użytkowników oraz interfejsy komunikacyjne z dostawcami PID i stronami ufającymi;
 - II. wyniki testów technicznych i ocen bezpieczeństwa;
 - III. ślady audytowe i zapisy logów z infrastruktury serwerowej eksploatowanej przez dostawcę portfela lub dostawcę PID w środowisku produkcyjnym — to jest w systemach obsługujących rzeczywistych użytkowników w autentycznych transakcjach, w odróżnieniu od środowisk testowych, pilotażowych lub referencyjnych — w tym systemów back-end do aktywacji jednostek portfela i zarządzania nimi, wydawania i unieważniania PID oraz poświadczeń, rejestrowania zdarzeń oraz interfejsów z innymi komponentami ekosystemu Portfela EUDI;
 - IV. ważne certyfikaty wydane w ramach GP-01 i GP-02 obejmujące rozwiązanie portfela lub deklarację dostawcy portfela, że procesy oceny i certyfikacji w ramach GP-01 i GP-02 są w toku;
 - V. zewnętrzne dowody uzasadnienia zaufania ocenione zgodnie z pkt 7.6
 - VI. oświadczenia, wyjaśnienia i demonstracje przedstawione przez personel dostawcy EUDI, dostawcy PID oraz Właściciela programu;
 - VII. wyniki działań próbkowania;
 - VIII. raporty z wcześniejszych ocen lub certyfikacji, w tym wszelkie oceny regulacyjne lub nadzorcze.
- 54 CAB dokumentuje uzyskane dowody i przechowuje je zgodnie z wymaganiami dotyczącymi prowadzenia zapisów określonymi w G-01, sekcja 5.10.

7.5 Proporcjonalność

55 Przy stosowaniu wymagań określonych w dokumentach WZ-03, WP-03 i WM-03 stosuje się następujące zasady proporcjonalności:

- I. Wszystkie wymagania wynikające z rozporządzenia wykonawczego Komisji (UE) 2015/1502, pkt 2.4, rozumie się jako współmierne do ryzyk na poziomie uzasadnienia zaufania <potwierdzanie tożsamości> „wysokim”, zgodnie z przepisem wprowadzającym tego punktu.
- II. Wszystkie wymagania wynikające z rozporządzenia wykonawczego Komisji (UE) 2024/2690 stosuje się z należyтым uwzględnieniem stopnia narażenia dostawcy Portfela EUDI lub dostawcy PID na ryzyka, jego wielkości i struktury jako podmiotu sektora publicznego oraz prawdopodobieństwa wystąpienia incydentów i ich dotkliwości, zgodnie z art. 2 ust. 2 tego rozporządzenia.
- III. W przypadku gdy CIR (UE) 2024/2690 przewiduje, że wymaganie techniczne lub metodyczne stosuje się „w stosownych przypadkach”, „w mających zastosowanie przypadkach” lub „w możliwym zakresie”, a dostawca Portfela EUDI / dostawca PID uznaje że nie ma uzasadnienia dla zastosowania lub są one niewykonalne, dostawca Portfela EUDI / dostawca PID dokumentuje swoje uzasadnienie w sposób wyczerpujący. CAB ocenia adekwatność i umocowanie takiego uzasadnienia.

56 CAB uwzględnia treść rejestru ryzyka (opartego na szablonie udostępnionym w G-04) przy określaniu głębokości i ukierunkowania działań oceniających, zwracając szczególną uwagę na ryzyka wynikające z integracji rozwiązania Portfela EUDI z polskimi krajowymi rejestrami tożsamości oraz rejestrem PESEL.

7.6 Akceptowalność i ponowne wykorzystanie dowodów uzasadnienia zaufania

57 *UWAGA 1: Zasady uznawania materiału dowodowego z zewnętrznych źródeł są określone w G-01, sekcja 5.3.*

58 Zgodnie z art. 13 ust. 1 lit. f) rozporządzenia wykonawczego Komisji (UE) 2024/2981 oraz załącznikiem VI do tego rozporządzenia CAB, w ramach oceny, ocenia akceptowalność dowodów uzasadnienia zaufania przedstawionych przez dostawcę PID, dostawcę Portfela EUDI lub właściciela programu.

- 59 Decyzja CAB o akceptowalności i dalszym ponownym wykorzystaniu dowodów uzasadnienia zaufania podejmowana jest zgodnie z ogólnymi zasadami określonymi w G-01, pkt 5.3, oraz zasadami szczegółowymi przedstawionymi poniżej.
- 60 Dowody uzasadnienia zaufania, jeżeli mają zastosowanie, mogą być przedstawione CAB jako dowód zgodności z wymaganiami dokumentów WZ-03 i WP-03, z zastrzeżeniem poniższych kryteriów oceny:
- I. certyfikaty zgodności wydane na zgodność z ISO/IEC 27001 przez jednostkę certyfikującą akredytowaną przez Polskie Centrum Akredytacji lub dowolną krajową jednostkę akredytującą w UE, zgodnie z PN-EN ISO/IEC 17021-1;
 - II. certyfikaty zgodności wydane na zgodność z ETSI EN 319 411-1 lub EN 319 411-2 dla kwalifikowanych dostawców usług zaufania, przez jednostkę oceniającą zgodność akredytowaną zgodnie z PN-EN ISO/IEC 17065 przez właściwą krajową jednostkę akredytującą;
 - III. certyfikaty zgodności lub raporty z oceny wydane w ramach europejskich lub krajowych programów certyfikacji cyberbezpieczeństwa (takich jak EUCC lub program oparty na EN 17640, jeżeli istnieją przepisy prawne przewidujące wzajemne uznawanie);
 - IV. inne raporty lub certyfikaty poświadczające, wydane według uznanych norm lub ram, o ile spełniają kryteria oceny określone w pkt 7.7
- 61 *UWAGA 2: Dalsze informacje o ponownym wykorzystaniu zewnętrznych dowodów uzasadnienia zaufania w planowaniu i realizacji audytu zawiera załącznik B.*

7.7 Kryteria oceny

- 62 CAB ocenia akceptowalność dowodów uzasadnienia zaufania zgodnie z metodyką określoną w załączniku VI do rozporządzenia wykonawczego Komisji (UE) 2024/2981 oraz kryteriami z załącznika II do tego rozporządzenia. Ocena obejmuje co najmniej następujące wymiary:
- I. **Kompetencje i bezstronność wystawcy.** CAB weryfikuje kompetencje zawodowe i bezstronność jednostki lub osoby, która wydała raport lub certyfikat poświadczający, zgodnie z pkt. 7.6. W przypadku jednostek certyfikujących weryfikacji podlega akredytacja według właściwej normy (PN-EN ISO/IEC 17021-1, PN-EN ISO/IEC 17065 lub równoważnej) udzielona przez krajową jednostkę akredytującą wyznaczoną na podstawie rozporządzenia (WE) nr 765/2008.

- II. **Adekwatność zakresu.** CAB weryfikuje, czy zakres dokumentacji poświadczającej obejmuje usługi, procesy, zabezpieczenia i systemy istotne dla wymagań ocenianych w ramach niniejszego programu certyfikacji.

PRZYKŁAD 1: Certyfikacja ISO/IEC 27001 poświadcza zgodność samego systemu zarządzania bezpieczeństwem informacji (procesów ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia SZBI); sama w sobie nie daje wystarczającego uzasadnienia zaufania, że poszczególne zabezpieczenia wybrane w deklaracji stosowania są zaprojektowane i działają na poziomie rygoru wymaganym przez niniejszy program. CAB przeprowadza zatem własną ocenę zaprojektowania i skuteczności operacyjnej konkretnych zabezpieczeń wymaganych przez serię dokumentów WM, nawet jeżeli certyfikat ISO/IEC 27001 został wydany.

- III. **Aktualność.** Dowody uzasadnienia zaufania muszą być aktualne w chwili oceny. Certyfikaty muszą znajdować się w okresie ważności. Raporty poświadczające muszą obejmować okres sprawozdawczy wystarczająco niedawny, aby dawać przekonanie, że opisane zabezpieczenia nadal funkcjonują. W przypadku gdy między końcem okresu sprawozdawczego a datą oceny występuje luka, CAB przeprowadza własną ocenę uzupełniającą okresu nieobjętego raportem.
- IV. **Rygor i głębokość oceny.** Stopień zaufania zapewniany przez dokumentację poświadczającą musi być współmierny do krytyczności wymagań, które obejmuje. CAB uwzględnia rygor zastosowanej metodyki oceny, głębokość przeprowadzonych badań oraz charakter wyrażonej opinii lub konkluzji poświadczającej.
- V. **Ustalenia i wyjątki.** CAB dokonuje przeglądu wszelkich ustaleń, zastrzeżeń, wyjątków lub uwag odnotowanych w dowodach uzasadnienia zaufania. W przypadku wystąpienia istotnych ustaleń CAB rozstrzyga, czy są one istotne dla wymagań niniejszego programu, a jeżeli tak — czy zostały odpowiednio zaadresowane.

63 *UWAGA 1: W przypadkach określonych w klauzulach II i III CAB dokumentuje zakres i wyniki wszelkich uzupełniających lub alternatywnych badań oraz zapewnia ich włączenie do zapisów certyfikacyjnych.*

64 *PRZYKŁAD 2: Zob. wynik przykładu 1. W przypadku PN-EN ISO/IEC 27001 CAB przeprowadza własną ocenę zaprojektowania i skuteczności operacyjnej konkretnych zabezpieczeń wymaganych przez dokumenty WZ-03, nawet jeżeli certyfikat ISO/IEC 27001 został wydany.*

8 Proces certyfikacji

8.1 Postanowienia ogólne

65 Proces certyfikacji GP-03 dzieli się na trzy główne fazy: fazę przygotowania i wniosku, fazę oceny oraz fazę certyfikacji. Każdą z faz opisano w poniższych podpunktach.

66 Metodykę oceny mającą zastosowanie do każdej fazy określono w rozdziale 7 niniejszego dokumentu. Proces certyfikacji prowadzony jest zgodnie z procedurami ustanowionymi przez CAB, na podstawie G-01 i G-05.

8.2 Faza przygotowania i wniosku

67 *UWAGA: Faza ta odzwierciedla PN-EN ISO/IEC 17065, pkt 7.2 i 7.3.*

68 Przed rozpoczęciem oceny od wnioskodawcy wymagane są następujące dokumenty i informacje:

- I. opis systemu eID, w tym struktury ładu korporacyjnego, zakresu usług oraz rozwiązań organizacyjnych dostawcy PID, dostawcy Portfela EUDI oraz — w stosownych przypadkach — Właściciela programu;
- II. dokumentacja wykazująca zgodność z wymaganiami WZ-03 i WP-03, w tym polityki, procedury, oceny ryzyka i zapisy istotne dla zakresu oceny;
- III. ważne certyfikaty wydane w ramach GP-01 i GP-02 obejmujące wersję (wersje) rozwiązania portfela objęte zakresem lub deklaracje, że procesy oceny i certyfikacji w ramach GP-01 i GP-02 są w toku zapis dotyczy także G-03 dla dostawcy PID;
- IV. wszelkie dostępne zewnętrzne dowody uzasadnienia zaufania (np. certyfikaty ISO/IEC 27001, raporty z audytów), które wnioskodawca zamierza przedstawić do wykorzystania zgodnie z pkt 7.6;
- V. wypełniony formularz wniosku udostępniany przez jednostkę CAB zgodnie z jej procedurami wewnętrznymi.

69 Wnioskodawca może złożyć formularz wniosku w ramach GP-03 odrębnie albo jako wniosek łączony obejmujący kilka programów certyfikacji w ramach Systemu Certyfikacji PL Portfela EUDI, zgodnie z G-01.

8.3 Faza oceny

70 *UWAGA: Faza ta odzwierciedla PN-EN ISO/IEC 17065, pkt 7.4.*

8.3.1 Spotkanie otwierające

71 Spotkanie otwierające odbywa się nie później niż 10 dni roboczych od otrzymania kompletnego wniosku i całej wymaganej dokumentacji. W spotkaniu otwierającym uczestniczą wszystkie strony zaangażowane w ocenę — wnioskodawca, przedstawiciele Właściciela programu oraz CAB.

72 Na spotkaniu otwierającym CAB uzgadnia z wnioskodawcą plan oceny, w tym zakres i harmonogram działań oceniających, podejście do ustalania zakresu polegania na zewnętrznych dowodach uzasadnienia zaufania oraz ustalenia dotyczące wizyt na miejscu i wywiadów.

8.3.2 Ocena

73 Ocena prowadzona jest zgodnie z metodyką oceny określoną w rozdziale 7 oraz mającymi zastosowanie ramami audytu WM-03. CAB dokumentuje wszystkie działania oceniające, uzyskane dowody i ustalenia w raporcie z oceny.

74 W przypadku gdy w trakcie oceny pojawią się istotne ustalenia, które mogą uniemożliwić pozytywną decyzję certyfikacyjną, CAB powiadamia o tym wnioskodawcę bez zbędnej zwłoki. Wnioskodawca może przedstawić dodatkowe informacje lub wyjaśnienia w odpowiedzi na takie ustalenia w terminie uzgodnionym na spotkaniu otwierającym.

75 Raport z oceny zawiera ogólną ocenę zgodności z każdym mającym zastosowanie wymaganie WZ-03, WP-03 i WM-03, ustalenie zakresu polegania na wszelkich wykorzystanych zewnętrznych dowodach uzasadnienia zaufania oraz rekomendację dotyczącą decyzji certyfikacyjnej.

8.4 Faza certyfikacji

76 *UWAGA: Faza ta odzwierciedla PN-EN ISO/IEC 17065, pkt 7.5–7.7 i 7.13.*

77 Po przeglądzie wyników oceny CAB podejmuje decyzję certyfikacyjną i informuje wnioskodawcę o jej wyniku w terminie 5 dni roboczych. Jeżeli decyzja certyfikacyjna jest pozytywna, certyfikat zgodności wydawany jest nie później niż 14 dni roboczych po podjęciu decyzji.

- 78 Odwołania i skargi rozpatrywane są zgodnie z postanowieniami ogólnymi zawartymi w G-01. Wnioskodawca może złożyć oświadczenie o braku sprzeciwu — w takim przypadku procedura publikacji, jeżeli ma zastosowanie, rozpoczyna się niezwłocznie po złożeniu oświadczenia.
- 79 Jeżeli decyzja certyfikacyjna jest negatywna, wnioskodawca ma 14 dni roboczych na wniesienie pisemnego odwołania do CAB. CAB rozpatruje odwołanie i wydaje decyzję ostateczną w terminie 14 dni roboczych od otrzymania sprzeciwu.

8.5 Nakłady na ocenę i certyfikację

- 80 Orientacyjną pracochłonność przeprowadzenia oceny i certyfikacji w ramach GP-03 przedstawiono w Tabeli 3. Szacunki te dotyczą certyfikacji początkowej; nakłady na działania nadzorcze i recertyfikacyjne określono odpowiednio w pkt 8.2 i 8.3.
- 81 Wartości ujęte w Tabeli 3 są wartościami maksymalnymi i planowanymi i mogą ulec zmianie na mocy porozumienia z Właścicielem programu.

Tabela 3 Planowana pracochłonność oceny i certyfikacji

Faza	Planowana pracochłonność CAB
Ocena	14 dni roboczych
Certyfikacja	10 dni roboczych

8.6 Postanowienia dodatkowe

- 82 Certyfikat zgodności jest ważny przez trzy lata od daty wydania.
- 83 CAB archiwizuje wszystkie dowody istotne dla certyfikacji przez okres określony w G-01, sekcja 5.10.
- 84 Wymiana informacji między jednostką CAB a wnioskodawcą jest zabezpieczana z użyciem najnowocześniejszych mechanizmów kryptograficznych zatwierdzonych przez właściciela programu. Wykaz mających zastosowanie mechanizmów zawiera G-03.

8.7 Certyfikat zgodności

- 85 Po pomyślnym zakończeniu oceny CAB wydaje certyfikat zgodności określający:
- I. przedmiot certyfikacji (system eID);

- II. zakres certyfikacji, z wyraźnym odesłaniem do każdego mającego zastosowanie dokumentu WZ-03, WP-03 i WM-03 oraz do właściwych norm lub specyfikacji technicznych, do których dokumenty te się odwołują;
 - III. nazwę dostawcy PID / dostawcy EUDI;
 - IV. wersję (wersje) rozwiązania portfela, do których system eID ma zastosowanie;
 - V. okres ważności certyfikatu (nieprzekraczający trzech lat);
 - VI. wszelkie warunki, ograniczenia lub wyjątki związane z certyfikatem.
- 86 CAB powiadamia Właściciela programu o wydanym certyfikacie w terminie pięciu dni roboczych od wydania, zgodnie z procedurą ustanowioną w G-03.
- 87 Przed wydaniem certyfikatu zgodności CAB weryfikuje, czy wnioskodawca posiada ważne certyfikaty wydane w ramach mających zastosowanie programów certyfikacji GP-01 i GP-02, obejmujące wersję (wersje) rozwiązania portfela podlegające ocenie GP-03. CAB nie wydaje certyfikatu zgodności GP-03, jeżeli którykolwiek z wymaganych certyfikatów GP-01 lub GP-02 nie istnieje, wygasł, został zawieszony lub cofnięty.

8.8 Nadzór

- 88 *UWAGA 1: Zasady realizacji działań w nadzorze są określone w G-01, sekcja 5.4.*
- 89 Przez cały okres ważności certyfikatu CAB prowadzi coroczne działania nadzorcze w celu weryfikacji, czy posiadacz certyfikatu nadal spełnia wymagania certyfikacyjne. Nadzór obejmuje co najmniej:
- I. przegląd istotnych zmian rozwiązania portfela, jego komponentów lub rozwiązań organizacyjnych dostawcy PID lub dostawcy Portfela EUDI, lub — w stosownych przypadkach — Ministerstwa Cyfryzacji, notyfikowanych jednostce CAB zgodnie z procedurami WZ-03-01 i WZ-03-02;
 - II. przegląd wszelkich incydentów lub naruszeń bezpieczeństwa notyfikowanych przez CAB zgodnie z WZ-03-01 i WZ-03-02;
 - III. przegląd wszelkich aktualizacji dokumentów podrzędnych WZ-03, WP-03 lub WM-03 i ich skutków dla programu certyfikacji GP-03;

- IV. ukierunkowane działania oceniające określone przez jednostkę CAB na podstawie rejestru ryzyka (opartego na szablonie udostępnionym w G-04) oraz wszelkich informacji zgromadzonych w okresie nadzoru;
- V. przegląd wyników działań monitorowania zgodności prowadzonych w okresie nadzoru przez dostawcę PID, dostawcę Portfela EUDI oraz — w stosownych przypadkach — Ministerstwo Cyfryzacji, zgodnie z G-01;
- VI. weryfikację, czy rozwiązanie portfela nadal posiada ważne certyfikaty w ramach mających zastosowanie programów certyfikacji GP-01 i GP-02 na podstawie G-01;
- VII. działania następcze w odniesieniu do wszelkich niezgodności, obserwacji lub warunków wcześniej zidentyfikowanych przez jednostkę CAB-CB, w celu weryfikacji skutecznego wdrożenia działań korygujących.
- 90 *UWAGA 2: Cykl życia certyfikacji przedstawiony w Tabeli 4 oraz działania w nadzorze mają zastosowanie przede wszystkim do certyfikacji usług w ramach programu GP-03; działania nadzorcze w odniesieniu do certyfikacji wyrobów są określone w mających zastosowanie dokumentach programów (tj. GP-01 i GP-02).*
- 91 8.8.1 CAB-CB musi prowadzić działania nadzorcze przez cały cykl życia certyfikacji, obejmujące co najmniej:
- 92 a) przeprowadzenie pełnej oceny przedmiotu oceny zgodności w ocenie początkowej i każdej ocenie recertyfikacyjnej, w tym wszelkich aktualizacji jego komponentów;
- 93 b) przeprowadzenie oceny podatności podczas oceny początkowej, każdej recertyfikacji oraz co najmniej co dwa lata w ramach działań nadzorczych. Ocena musi obejmować co najmniej zmiany przedmiotu certyfikacji oraz środowiska zagrożeń od czasu poprzedniej oceny;
- 94 c) wykonanie dodatkowych działań, takich jak testy penetracyjne, w przypadku wzrostu poziomu ryzyka lub pojawienia się nowych zagrożeń.

Tabela 4 3-letni cykl życia certyfikatu w G-03

Rok	Rodzaj działania	Działania obowiązkowe
0	Certyfikacja początkowa	- Pełna ocena rozwiązania portfela, w tym ocena podatności - Ocena procesów utrzymania, z wyłączeniem ich skuteczności operacyjnej - Przyznanie certyfikacji i rozpoczęcie 3-letniego cyklu

Rok	Rodzaj działania	Działania obowiązkowe
1	Nadzór	- Ocena skuteczności operacyjnej procesów utrzymania - Co najmniej kontrola wersji, aktualizacje, zarządzanie podatnościami - Ocena zmian wpływających na bezpieczeństwo rozwiązania
2	Nadzór	- Ocena podatności całego rozwiązania - Ocena skuteczności operacyjnej procesów utrzymania — co najmniej kontrola wersji, aktualizacje, zarządzanie podatnościami - Ocena zmian wpływających na bezpieczeństwo rozwiązania
3	Recertyfikacja	- Pełna ponowna ocena. - Pełna ocena przedmiotu certyfikacji, w tym ocena podatności - Ocena uproszczona dla cech/procesów, które nie uległy zmianie, w tym funkcji przeprowadzania aktualizacji każdego komponentu programowego - Ocena procesów utrzymania, w tym ich skuteczności operacyjnej - Przyznanie nowej certyfikacji

95 Każde działanie nadzorcze przeprowadzane jest w ciągu 12 miesięcy od wydania certyfikatu, a następnie w ciągu 12 miesięcy od poprzedniego działania nadzorczego. Recertyfikacja przeprowadzana jest w ciągu 12 miesięcy po ostatnim działaniu nadzorczym.

8.9 Recertyfikacja

96 Recertyfikację wszczyna się przed upływem ważności bieżącego certyfikatu; przebiega ona zgodnie z procesem certyfikacji początkowej określonym w rozdziale 8. Recertyfikacja może opierać się na dowodach uzasadnienia zaufania pochodzących z działań nadzorczych prowadzonych w okresie ważności, a CAB może odpowiednio ograniczyć zakres swoich działań oceniających, zgodnie z pkt 7.6.

97 Recertyfikacja jest również wymagana w przypadku wystąpienia poważnej zmiany w systemie identyfikacji elektronicznej, w tym zmiany wersji rozwiązania portfela, jeżeli nowa wersja nie jest objęta istniejącym certyfikatem; zmiany struktury organizacyjnej dostawcy PID lub jego relacji z Ministerstwem Cyfryzacji; lub istotnej zmiany ram zaufania ustanowionych w G-03.

98 Wszystkie odpowiednie działania związane z recertyfikacją podejmowane są przez dostawcę PID i właściwe jednostki CAB w sposób terminowy. Wnioskodawca powiadamia jednostkę CAB o potrzebie recertyfikacji nie później niż sześć miesięcy przed upływem ważności bieżącego certyfikatu.

8.10 Zawieszenie i cofnięcie

99 CAB zawiesza certyfikat GP-03 w następujących okolicznościach:

- I. dostawca Portfela EUDI lub dostawca PID nie wdroży działań korygujących w uzgodnionym terminie po niezgodności zidentyfikowanej w trakcie nadzoru;
- II. stanowiący warunek wstępny certyfikat GP-01 lub GP-02 dostawcy Portfela EUDI zostaje zawieszony;
- III. odnotowany zostaje znaczący incydent lub naruszenie bezpieczeństwa, które może wpłynąć na zgodność — do czasu rozstrzygnięcia oceny skutków;
- IV. dostawca Portfela EUDI lub dostawca PID nie współpracuje przy działaniach nadzorczych lub nie zapewnia do nich dostępu.

100 *UWAGA — Termin wdrożenia działań korygujących, o którym mowa w pierwszej przesłance zawieszenia, uzgadniany jest na piśmie między jednostką CAB a dostawcą PID w chwili notyfikacji niezgodności. CAB określa odpowiedni termin, uwzględniając charakter i wagę niezgodności, zgodnie z postanowieniami G-05. CAB dokumentuje uzgodniony termin w raporcie z nadzoru.*

101 Okres zawieszenia nie przekracza 42 dni. Jego przedłużenie wymaga decyzji właściciela programu, jednak w żadnym przypadku nie może przekroczyć stu dni. Okres zawieszenia nie wpływa na okres ważności certyfikatu. CAB cofa certyfikat GP-03 w następujących okolicznościach:

- I. dostawca EUDI lub dostawca PID nie usunie w terminie wyznaczonym przez jednostkę CAB przyczyn, które doprowadziły do zawieszenia;
- II. stwierdzona zostanie potwierdzona niezgodność, której nie da się usunąć w rozsądnym terminie;

102 CAB-CB zakończy certyfikację na wniosek, odpowiednio dostawcy portfela lub dostawcy PID.

103 We wszystkich przypadkach zawieszenia, zakończenia lub cofnięcia CAB bez zbędnej zwłoki powiadamia Właściciela programu. Właściciel

programu aktualizuje rejestr certyfikatów zgodnie z obowiązkami określonymi w G-03.

8.11 Skutki zmian certyfikatów GP-01 / GP-02

104 W przypadku zawieszenia certyfikatu GP-01 lub GP-02 dostawcy Portfela EUDI CAB dla GP-03:

- I. wszczyna ocenę skutków w celu ustalenia, czy zawieszenie wpływa na zgodność certyfikowanego systemu eID z wymaganiami WZ-03 i WP-03;
- II. jeżeli ocena skutków wykaże, że zgodność jest istotnie naruszona — zawiesza certyfikat GP-03 do czasu rozwiązania problemu;
- III. jeżeli ocena skutków wykaże, że zgodność nie jest istotnie naruszona — dokumentuje uzasadnienie i kontynuuje monitorowanie;
- IV. w przypadku cofnięcia certyfikatu GP-01 lub GP-02 dostawcy Portfela EUDI certyfikat GP-03 zostaje niezwłocznie zawieszony do czasu recertyfikacji po przywróceniu certyfikatu GP-01 lub GP-02.

9 Działania związane z certyfikatem najwyższego poziomu

9.1 Wydanie certyfikatu najwyższego poziomu

105 CAB-CB, która przeprowadza certyfikację usług dostawcy portfela w ramach programu certyfikacji GP-03, rozpoczyna działania dotyczące certyfikatu najwyższego poziomu po spełnieniu następujących warunków:

- I. dostawca portfela ma prawnie wiążącą umowę z jednostką CAB-CB, zawierającą warunki i podstawę wydania oraz utrzymywania certyfikatu najwyższego poziomu;
- II. dostawca portfela przedkłada w odpowiednim czasie wszystkie ważne certyfikaty lub deklaracje zgodności wydane w ramach programów certyfikacji GP-01, GP-02 i GP-03, w tym certyfikat uzyskany przez dostawcę PID;
- III. dostawca portfela przedkłada ważne certyfikaty wydane w ramach programu certyfikacji EUCC dla odpowiednich komponentów rozwiązania Portfela EUDI, tj. WSCD i WSCA.

106 CAB-CB analizuje przedłożoną dokumentację i sprawdza, czy spełnia ona wymagania określone we wszystkich programach certyfikacji objętych zakresem. CAB-CB wydaje certyfikat wyłącznie wtedy, gdy wszystkie sprawdzenia zakończą się pomyślnie.

107 CAB-CB kończy proces nie później niż w terminie 5 dni roboczych, licząc d przedłożenia ostatniego certyfikatu.

9.2 Nadzór

108 CAB prowadzi działania nadzorcze w odniesieniu do certyfikatu najwyższego poziomu przez cały cykl życia certyfikacji, obejmujące co najmniej:

- I. sprawdzanie statusu ważności wszystkich odpowiednich certyfikatów lub deklaracji zgodności, na których opiera się certyfikat najwyższego poziomu;
- II. uwzględnianie wyników pełnej oceny przedmiotu certyfikacji w ocenach początkowych i każdej recertyfikacji, w tym wszelkich aktualizacji wyrobów, ich części lub usług;

- III. uwzględnianie wyników oceny podatności podczas ocen początkowych, każdej recertyfikacji oraz co najmniej co dwa lata w ramach działań nadzorczych. Ocena obejmuje co najmniej zmiany przedmiotu certyfikacji oraz środowiska zagrożeń od czasu poprzedniej oceny;
- IV. uwzględnianie wyników działań dodatkowych, takich jak testy penetracyjne, w przypadku wzrostu poziomu ryzyka lub pojawienia się nowych zagrożeń.

109 CAB uwzględnia wyniki innych działań nadzorczych dotyczących przedmiotu certyfikacji. W przypadku gdy działania te prowadzi CAB niebędąca wystawcą certyfikatu najwyższego poziomu, wszystkie odpowiednie wyniki udostępniane są pierwszej CAB bez zbędnej zwłoki.

110 Jeżeli wszystkie odpowiednie wyniki są niewystarczające do zakończenia nadzoru, CAB decyduje o dodatkowych ocenach o określonym zakresie i pracochłonności.

111 Do interpretacji wyników nadzoru stosuje się postanowienia ogólne zawarte w G-01, pkt 5.4.

9.3 Zmiany przedmiotu certyfikacji najwyższego poziomu

112 Stosuje się postanowienia ogólne zawarte w G-01, pkt 5.6.

9.4 Zawieszenie, zakończenie i cofnięcie certyfikatu

113 Stosuje się postanowienia ogólne zawarte w G-01, pkt 5.8.

10Postanowienia końcowe

10.1 Ustawodawstwo krajowe

- 114 Program certyfikacji GP-03 jest ustanowiony na podstawie ustawodawstwa krajowego wdrażającego rozporządzenie eIDAS w Polsce, zgodnie z aktami prawnymi wymienionymi w rozdziale 3 niniejszego dokumentu

10.2 Umowy certyfikacyjne

- 115 CAB zawiera z wnioskodawcą umowę certyfikacyjną opartą na postanowieniach GP-03. Właściciel programu może określić postanowienia umowne.
- 116 Umowa certyfikacyjna nie może zawierać postanowień, które utrudniałyby prawidłowy przebieg certyfikacji lub przekazywanie między wnioskodawcą a CAB informacji istotnych dla decyzji certyfikacyjnej.

10.3 Koszty

- 117 Wszystkie koszty opierają się na rzeczywistych nakładach certyfikacyjnych.
- 118 Do GP-03 stosuje się ogólne zasady wynagradzania kosztów i wydatków określone w G-01.

Załącznik A (normatywny) — Przypisanie wymagań do dokumentów podrzędnych

119 *UWAGA: Niniejszy załącznik zawiera normatywne przypisanie wymagań prawnych — wynikających z aktów wymienionych w rozdziale 3 — do dokumentów podrzędnych GP-03. Przypisanie to stanowi podstawę zakresu oceny określonego w pkt 7.2 niniejszego dokumentu. Wymagania mające zastosowanie wyłącznie do dostawcy portfela przypisane są do WZ-03-03 i nie są odrębnie wymienione w niniejszym załączniku; wynikają one z tych samych aktów prawnych, do których odesłano poniżej.*

A.1 Wymagania z rozporządzenia (UE) nr 910/2014 (eIDAS)

Identyfikator	Wymaganie
REQ-910-01	EUDIW umożliwia użytkownikom bezpieczne zarządzanie PID i EAA pod wyłączną kontrolą użytkownika. [art. 5a ust. 4 lit. a)] → WP-03-02, WP-03-03
REQ-910-02	EUDIW umożliwia użytkownikom pobranie swoich danych i konfiguracji. [art. 5a ust. 4 lit. f)] → WP-03-02
REQ-910-03	EUDIW spełnia poziom uzasadnienia zaufania „wysoki”. [art. 5a ust. 5 lit. d)] → WZ-03-01, WZ-03-02, WP-03-01, WP-03-03
REQ-910-04	PID jednoznacznie reprezentuje osobę fizyczną. [art. 5a ust. 5 lit. f)] → WP-03-01
REQ-910-05	Dane osobowe związane z dostarczaniem EUDIW przechowywane logicznie oddzielnie. [art. 5a ust. 14] → WZ-03-01, WZ-03-02
REQ-910-06	Użytkownicy poddawani onboardingowi z użyciem środków eID o poziomie uzasadnienia zaufania „wysokim”. [art. 5a ust. 24] → WP-03-01, WP-03-03

A.2 Wymagania z CIR (UE) 2015/1502

Identyfikator	Wymaganie
REQ-1502-2.1	Wymagania dotyczące rejestracji na poziomie uzasadnienia zaufania „wysokim”. [załącznik, pkt 2.1] → WP-03-01, WP-03-03
REQ-1502-2.2	Zarządzanie środkami eID na poziomie uzasadnienia zaufania „wysokim”. [załącznik, pkt 2.2] → WP-03-01, WP-03-02, WP-03-03
REQ-1502-2.4.1	Status prawny, zdolność finansowa, outsourcing. [załącznik, pkt 2.4.1] → WZ-03-01, WZ-03-02
REQ-1502-2.4.2	Publikowane komunikaty i informacje dla użytkowników. [załącznik, pkt 2.4.2] → WZ-03-01, WZ-03-02

Identyfikator	Wymaganie
REQ-1502-2.4.3	System zarządzania bezpieczeństwem informacji. [załącznik, pkt 2.4.3] → WZ-03-01, WZ-03-02
REQ-1502-2.4.4	Prowadzenie zapisów. [załącznik, pkt 2.4.4] → WZ-03-01, WZ-03-02
REQ-1502-2.4.5	Obiekty i personel. [załącznik, pkt 2.4.5] → WZ-03-01, WZ-03-02
REQ-1502-2.4.6	Zabezpieczenia techniczne. [załącznik, pkt 2.4.6] → WZ-03-01, WZ-03-02
REQ-1502-2.4.7	Zgodność i audyt. [załącznik, pkt 2.4.7] → WZ-03-01, WZ-03-02

A.3 Wymagania z CIR (UE) 2024/2977

Identyfikator	Wymaganie
REQ-2977-3	Wymagania techniczne dotyczące wydawania PID. [art. 3] → WZ-03-02, WP-03-01
REQ-2977-5	Zarządzanie statusem ważności PID i unieważnianie. [art. 5] → WZ-03-02, WP-03-01

A.4 Wymagania z CIR (UE) 2024/2979

Identyfikator	Wymaganie
REQ-2979-3,4	Wydawanie poświadczeń jednostki portfela. [art. 3, 4] → WP-03-02
REQ-2979-6,7	Obowiązki dostawcy portfela — informowanie użytkowników, unieważnianie. [art. 6, 7] → WP-03-02
REQ-2979-9,13	Rejestrowanie zdarzeń i przenoszenie danych. [art. 9, 13] → WP-03-02

A.5 Wymagania z CIR (UE) 2024/2981

Identyfikator	Wymaganie
REQ-2981-4	Ocena ryzyka i kryteria bezpieczeństwa. [art. 4, 8] → WZ-03-01, WZ-03-02
REQ-2981-5	Zarządzanie incydentami i podatnościami. [art. 5] → WZ-03-01, WZ-03-02
REQ-2981-8(3)(g)	Korzystanie z aktualnie certyfikowanej wersji rozwiązania portfela. [art. 8 ust. 3 lit. g)] → WZ-03-01, WP-03-02
REQ-2981-19	Przechowywanie zapisów. [art. 19] → WZ-03-01, WZ-03-02

A.6 Wymagania z CIR (UE) 2024/2690

Identyfikator	Wymaganie
REQ-2690-Annex	Techniczne i metodyczne wymagania cyberbezpieczeństwa. [załącznik, pkt 1–13] → WZ-03-01, WZ-03-02, WZ-03-03

Załącznik B Ramy audytu

B.1 Cel

- 120 W niniejszym aneksie określono wspólne ramy planowania, przeprowadzania i dokumentowania audytów cyberbezpieczeństwa wykonywanych przez jednostkę oceniającą zgodność w ramach programu certyfikacji GP-03.
- 121 W aneksie odwzorowano podejście audytowe normy ETSI EN 319 403-1 na strukturę Systemu Certyfikacji PL Portfela EUDI, które stanowi spójną podstawę dla wszystkich dokumentów WM-03-0x dotyczących poszczególnych kryteriów.
- 122 W dokumencie określono uniwersalne zasady audytu, metody, próbkowanie, kompetencje, gromadzenie dowodów, raportowanie i działania następcze po działaniach korygujących. W dokumencie nie zdefiniowano sposobu testowania poszczególnych wymagań wynikających ze specyfikacji technicznych, w tym ETSI EN 319 401, aktów wykonawczych lub innych kryteriów. Te szczegółowe metody są określone w odrębnych dokumentach WM dotyczących poszczególnych kryteriów.
- 123 Jeżeli dokument WM-03-xx dotyczący poszczególnych kryteriów zawiera dodatkowe lub bardziej szczegółowe wymagania audytowe, wymagania te muszą być stosowane łącznie z niniejszymi ramami.

B.2 Zakres

- 124 Niniejsze ramy mają zastosowanie do audytów cyberbezpieczeństwa przeprowadzanych w ramach etapu oceny GP-03. Przedmiotem certyfikacji jest system identyfikacji elektronicznej oraz powiązane usługi i procesy.
- 125 Ramy mają zastosowanie do:
- 126 audytów oceny początkowej;
- 127 corocznych audytów nadzoru;
- 128 audytów ponownej oceny;
- 129 audytów specjalnych uruchamianych w związku z istotnymi zmianami, incydentami, skargami lub innymi uzasadnionymi informacjami; audytów

usług zleconych na zewnątrz, procesów podzleconych lub odrębnie ocenianych komponentów w zakresie istotnym dla wymagań certyfikacyjnych.

- 130 Ramy muszą być stosowane w zakresie odpowiednim do charakteru, ryzyka i zakresu czynności oceny.
- 131 Zakres oceny nie może być ograniczany wyłącznie z tego powodu, że dostępne jest zewnętrzny materiał dowodowy uzasadnienia zaufania. Zewnętrzny materiał dowodowy może ograniczyć zakres własnych czynności audytowych CAB wyłącznie po udokumentowanym ustaleniu polegania na tym materiale dowodowym.

B.3 Odniesienia, terminy i role

B.3.1 Odniesienia

- 132 ISO/IEC 17065 — Ocena zgodności — Wymagania dla jednostek certyfikujących wyroby, procesy i usługi;
- 133 ETSI EN 319 403-1 — Ocena zgodności dostawców usług zaufania — Wymagania dla jednostek oceniających zgodność dokonujących oceny dostawców usług zaufania;
- 134 G-01. System certyfikacji PL Portfela EUDI;
- 135 G-05. Wymagania akredytacyjne dla jednostek oceniających zgodność (CAB);
- 136 GP-03. System certyfikacji eID;
- 137 mające zastosowanie dokumenty WZ-03, WP-03 oraz dokumenty WM-03 dotyczące poszczególnych kryteriów.

B.3.2 Role i odpowiedzialności

- 138 Właściwe role i odpowiedzialności przedstawiono w Tabeli .

Tabela 1 Role i odpowiedzialności w ramach audytu cyberbezpieczeństwa

Rola	Odpowiedzialność
CAB	Jednostka certyfikująca akredytowana i upoważniona do wykonywania czynności oceny zgodności i certyfikacji w ramach GP-03.

Rola	Odpowiedzialność
Wnioskodawca / posiadacz certyfikatu	Podmiot, który ubiega się o certyfikację GP-03 lub ją posiada.
Dostawca	Dostawca PID, dostawca Portfela EUDI, dostawca eID* lub dostawca usług wspierających**, których rozwiązania są objęte zakresem audytu. *dostawca eID jest rolą realizowaną przez rolę dostawcy PID albo dostawcy portfela **w niniejszej edycji PL Portfela EUDI role te nie podlegają ocenie ani późniejszym czynnościom certyfikacyjnym
Przedmiot certyfikacji	System identyfikacji elektronicznej i powiązane usługi zdefiniowane w GP-03.
Zespół audytowy	Co najmniej jeden audytor wyznaczony przez CAB lub jego podwykonawcę, wspierany w razie potrzeby przez ekspertów technicznych.
Kierownik zespołu audytowego	Audytor odpowiedzialny za zarządzanie audytem i raportowanie ustaleń do CAB.
Ekspert techniczny	Osoba dostarczająca zespołowi audytowemu wiedzy specjalistycznej, która nie działa samodzielnie jako audytor.

B.3.3 Terminy specyficzne dla ram audytu cyberbezpieczeństwa

139 Zastosowanie mają terminy i ich definicje przedstawione w Tabeli 2.

Tabela 2 Terminy i definicje

Termin	Definicja
Kryteria audytu	Mające zastosowanie wymagania z dokumentów serii G, GP, WZ, WP i WM, aktów prawnych, norm i specyfikacji.
Obiektywne dowody	Weryfikowalne informacje potwierdzające spełnienie lub niespełnienie kryterium audytu.
Zewnętrzny materiał dowodowy uzasadnienia zaufania	Certyfikat, raport, wynik oceny lub inny materiał dowodowy wytworzony poza bieżącą oceną GP-03 i przedłożony w celu ewentualnego polegania na nim.

B.4 Ogólne zasady audytu

140 Audyty muszą być planowane i przeprowadzane w sposób zapewniający bezstronność i spójność oraz chroniący informacje poufne.

141 Wnioski z audytu muszą opierać się na wystarczających i odpowiednich obiektywnych dowodach.

- 142 Głębokość i zakres czynności audytowych muszą być proporcjonalne do ryzyka, krytyczności wymagania, dojrzałości właściwych zabezpieczeń oraz wyników poprzednich audytów.
- 143 Zespół audytowy nie może narzucać określonej implementacji ani formatu dokumentacji, chyba że kryteria audytu wyraźnie tego wymagają.
- 144 Oświadczenia i wyjaśnienia muszą być w razie potrzeby potwierdzone zapisami, obserwacjami, wywiadami, wynikami testów lub innymi obiektywnymi dowodami.
- 145 Zespół audytowy musi ocenić zaprojektowanie i skuteczność operacyjną zabezpieczeń, jeżeli mające zastosowanie wymaganie dotyczy zarówno ich istnienia, jak i funkcjonowania.
- 146 Audyt musi uwzględniać rejestr ryzyka prowadzony przez dostawcę Portfela EUDI lub przez Właściciela Programu oraz inne informacje o ryzyku istotne dla przedmiotu certyfikacji przy doborze ścieżek audytu, próbek, lokalizacji i technicznych obszarów szczególnej uwagi.

B.5 Cele, zakres i czas audytu

B.5.1 Cele audytu

- 147 Dla każdego audytu CAB musi określić cele odpowiednie do czynności oceny.
- 148 *UWAGA: Cele mogą obejmować:*
- *ocenę zgodności z wymaganiami mającymi zastosowanie do zatwierdzonego zakresu;*
 - *sprawdzenie, czy zabezpieczenia są wdrożone i działają skutecznie;*
 - *potwierdzenie ciągłej zgodności podczas nadzoru;*
 - *ocenę wpływu istotnej zmiany lub incydentu;*
 - *śledzenie usuwania wcześniej wykrytych niezgodności;*
 - *uzyskanie dowodów wymaganych do ponownej oceny, rozszerzenia, ograniczenia lub innej decyzji w ramach programu.*

B.5.2 Zakres audytu

- 149 Zakres audytu musi obejmować, stosownie do przypadku:

- część systemu identyfikacji elektronicznej i powiązanych usług podlegającą ocenie;
- organizacje wnioskodawcy i jednostki organizacyjne objęte audytem;
- wymagania WZ-03, WP-03 i WM-03 oraz ich wersje objęte kryteriami audytu;
- procesy, systemy, komponenty, interfejsy, przepływy danych i środowiska operacyjne;
- lokalizacje fizyczne i logiczne;
- działania zlecone na zewnątrz i podzlecone;
- okres, z którego mają być wybierane zapisy i próbki;
- wszelkie zaakceptowane ograniczenia lub wyłączenia wraz z ich uzasadnieniem.

150 Zakres i granice muszą być na tyle jednoznaczne, aby uniknąć niejasności co do organizacji, usług, procesów, systemów i lokalizacji podlegających audytowi.

151 Jeżeli usługi zlecone na zewnątrz lub podzlecone są istotne dla spełnienia wymagań certyfikacyjnych, zakres audytu musi obejmować te usługi albo należy uzyskać wystarczające równoważne zapewnienie ich dotyczące.

B.5.3 Czas audytu

152 CAB musi przeznaczyć wystarczający czas na przygotowanie, przegląd dowodów, czynności audytowe, raportowanie i działania następcze. Określając czas audytu, CAB musi uwzględnić co najmniej:

- liczbę i złożoność mających zastosowanie wymagań;
- wielkość i złożoność przedmiotu certyfikacji oraz uczestniczących organizacji dostawców;
- liczbę lokalizacji, systemów, interfejsów i usług zleconych na zewnątrz;
- różnorodność i wolumen transakcji lub procesów powtarzalnych;
- wykorzystanie automatyzacji, kryptografii, biometrii, zdalnego onboarding lub innych technologii specjalistycznych;
- wyniki poprzednich ocen, incydenty i zmiany;

- dostępność i akceptowalność zewnętrznych dowodów uzasadnienia zaufania;
 - potrzebę specjalistycznej wiedzy technicznej;
 - wykorzystanie technik na miejscu i technik zdalnych.
- 153 CAB musi udokumentować określenie i uzasadnienie czasu audytu.
- 154 *UWAGA: Wytyczne do określenia czasu audytu dla audytu systemów zarządzania znajdują się w normie PN-EN ISO/IEC 27006-1 „Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji - Część 1: Postanowienia ogólne”, Załącznik D.*
- 155 Ograniczenia biznesowe lub harmonogramowe nie mogą skracać czasu audytu poniżej poziomu niezbędnego do uzyskania wystarczających i odpowiednich dowodów.

B.6 Planowanie audytu i spotkanie otwierające

- 156 CAB musi przygotować plan audytu w oparciu o cele, zakres, ryzyko, dostępne dowody i wymagania kompetencyjne.
- 157 Plan audytu musi określać co najmniej:
- cele, zakres i kryteria audytu;
 - członków zespołu audytowego i ich role;
 - terminy, lokalizacje, harmonogram i tryb czynności audytowych;
 - planowane ścieżki audytu i główne próbki;
 - wywiady, obserwacje i czynności techniczne;
 - wykorzystanie technik zdalnych i rozwiązania w zakresie bezpieczeństwa;
 - ustalenia dotyczące spotkania otwierającego, spotkań postępowych i spotkania zamykającego;
 - ustalenia dotyczące raportowania i komunikacji.
- 158 Plan audytu musi zostać uzgodniony z wnioskodawcą lub posiadaczem certyfikatu bez przenoszenia odpowiedzialności za koncepcję audytu na strony audytowane.

- 159 Spotkanie inauguracyjne lub otwierające musi potwierdzić zakres, harmonogram, odpowiedzialności, kanały komunikacji, ustalenia dotyczące dostępu, podejście do polegania na dowodach oraz sposób postępowania z istotnymi ustaleniami.
- 160 Zmiany planu w trakcie audytu muszą być dokumentowane i komunikowane właściwym stronom.

B.7 Metody i techniki audytu

- 161 CAB musi dobrać odpowiednią kombinację metod dla każdej czynności oceny.
- 162 *UWAGA: Dokumenty WM-03-0x dotyczące poszczególnych kryteriów mogą wymagać zastosowania określonych metod.*

B.7.1 Przegląd dokumentacji

- 163 *UWAGA: Przegląd dokumentacji może obejmować polityki, procedury, oświadczenia o praktykach, umowy, oceny ryzyka, opisy architektury, specyfikacje techniczne, konfiguracje, zapisy, logi, raporty z audytów wewnętrznych, przeglądy zarządzania, raporty z testów oraz dowody z wcześniejszych ocen.*
- 164 Przegląd dokumentacji musi służyć zrozumieniu koncepcji audytowanych rozwiązań oraz przygotowaniu kolejnych ścieżek audytu.

B.7.2 Wywiady

- 165 Wywiady muszą być prowadzone z personelem, którego role i odpowiedzialności są istotne dla zakresu audytu. Pytania muszą zmierzać do ustalenia rzeczywistej praktyki, odpowiedzialności, kompetencji i świadomości oraz muszą być w stosownych przypadkach potwierdzane.

B.7.3 Obserwacja i inspekcja

- 166 *UWAGA: Obserwacja może obejmować procesy, obiekty, zabezpieczenia, działanie systemów, czynności administracyjne i demonstracje techniczne. Inspekcja może być przeprowadzana na miejscu lub poprzez kontrolowany dostęp zdalny.*
- 167 Zespół audytowy musi uzgodnić ustalenia dotyczące dostępu, rejestrowania, zrzutów ekranu, kopiowania i poufności przed rozpoczęciem czynności inspekcyjnych.

- 168 Czynności audytowe muszą unikać zbędnych zakłóceń i nie mogą wprowadzać niedopuszczalnego ryzyka dla usług produkcyjnych ani danych osobowych.

B.7.4 Analiza zapisów, logów i transakcji

- 169 *UWAGA: Zespół audytowy może analizować logi, ścieżki audytu, zapisy transakcji, zapisy zmian, zapisy incydentów i inne dowody operacyjne w celu potwierdzenia wykonania, autoryzacji, identyfikowalności, integralności i skuteczności właściwych procesów.*

B.7.5 Testowanie i weryfikacja techniczna

- 170 *UWAGA: Weryfikacja techniczna może obejmować nadzorowane demonstracje, przegląd konfiguracji, wykonanie przypadków testowych, ponowne wykonanie, weryfikację interfejsów lub przegląd specjalistycznych testów bezpieczeństwa.*
- 171 Testy inwazyjne muszą być odrębnie autoryzowane i wykonywane przez kompetentny personel w warunkach kontrolowanych.

B.7.6 Techniki audytu zdalnego

- 172 *UWAGA: Techniki zdalne mogą być stosowane, jeżeli dostarczają dowodów o wystarczającej wiarygodności i kompletności oraz są dozwolone przez mający zastosowanie program i kryteria.*
- 173 Plan musi określać narzędzia, uwierzytelnianie, bezpieczeństwo transmisji, zasady rejestrowania oraz rozwiązywania awaryjne stosowane w zdalnych czynnościach audytowych.
- 174 Jeżeli techniki zdalne nie dostarczają wystarczających dowodów, zespół audytowy musi przeprowadzić dodatkowe czynności na miejscu lub czynności alternatywne.

B.8 Dowody audytowe i próbkowanie

B.8.1 Wystarczalność i odpowiedniość

- 175 Zespół audytowy musi uzyskać wystarczające i odpowiednie dowody na poparcie każdego wniosku z audytu.
- 176 Dowody muszą być istotne dla wymagania, wiarygodne co do pochodzenia i metody, wystarczająco aktualne oraz identyfikowalne w odniesieniu do audytowanego zakresu.

- 177 Brak określonego dokumentu nie może sam w sobie stanowić o niezgodności, chyba że kryterium wymaga tego dokumentu. I odwrotnie — samo istnienie dokumentacji nie może stanowić o skuteczności operacyjnej.

B.8.2 Próbkowanie

- 178 Próbkowanie może być stosowane, gdy zbadanie każdego przypadku jest niewykonalne. Próbkowanie musi być oparte na ryzyku, udokumentowane i odpowiednie do celu audytu.
- 179 *UWAGA: Przy doborze próby należy uwzględnić:*
- *procesy wysokiego ryzyka i procesy krytyczne;*
 - *różne warianty procesów i technologie;*
 - *przypadki zakończone powodzeniem, nieudane, odrzucone, wyjątkowe i eskalowane;*
 - *incydenty, skargi, anomalie i wskaźniki oszustw;*
 - *różne okresy, lokalizacje, systemy, dostawców i zespoły operacyjne;*
 - *niedawne zmiany oraz wersje oprogramowania lub konfiguracji;*
 - *elementy dobierane zarówno selektywnie, jak i nieselektywnie.*
- 180 CAB musi udokumentować populację, metodę doboru, wielkość próby, wybrane elementy oraz ograniczenia próby.

B.8.3 Wiele lokalizacji

- 181 Podejście wielolokalizacyjne oparte na próbkowaniu może być stosowane wyłącznie wtedy, gdy właściwe lokalizacje działają pod wspólną kontrolą oraz w ramach wspólnego systemu zarządzania i przeglądów.
- 182 Dobór lokalizacji musi uwzględniać różnice w wielkości, działalności, technologii, ryzyku, wymaganiach prawnych, praktykach pracy, podwykonawstwie oraz interakcji z systemami krytycznymi lub wrażliwymi.
- 183 Lokalizacje o znaczącym ryzyku lub istotnych różnicach muszą zostać objęte programem audytu.
- 184 Ustalenie w jednej lokalizacji musi zostać ocenione pod kątem możliwego wpływu systemowego na inne lokalizacje.

B.9 Zewnętrzny materiał dowodowy uzasadnienia zaufania

- 185 Dozwala się wykorzystanie zewnętrznego materiału dowodowego uzasadnienia zaufania może być wykorzystywane w celu ograniczenia powielania czynności oceny, jednak wyłącznie po udokumentowanej ocenie przeprowadzonej zgodnie z GP-03. CAB pozostaje w pełni odpowiedzialna za swoje wnioski z oceny i decyzję certyfikacyjną.

B.9.1 Ocena akceptowalności

- 186 Dla każdego elementu zewnętrznego materiału dowodowego uzasadnienia zaufania Zespół audytowy musi ocenić co najmniej:
- kompetencje, niezależność i — w stosownych przypadkach — akredytację wystawcy;
 - adekwatność zakresu i jego zgodność z bieżącym przedmiotem certyfikacji;
 - aktualność i ciągłą ważność;
 - rygor i głębokość zastosowanej metody;
 - ustalenia, zastrzeżenia, wyjątki i ograniczenia;
 - okres, wersje, lokalizacje, systemy i zabezpieczenia objęte dowodami;
 - potrzebę uzupełniających czynności audytowych.

B.9.2 Wykorzystanie zewnętrznego materiału dowodowego uzasadnienia zaufania w planowaniu i realizacji audytu

- 187 Zespół audytowy musi ocenić, w jakim stopniu zewnętrzny materiał dowodowy uzasadnienia zaufania wspiera mające zastosowanie kryteria audytu, oraz musi wskazać wszelkie wymagania, aspekty lub okresy, które nie są wystarczająco objęte tymi dowodami.
- 188 Na podstawie tej oceny zespół audytowy musi określić uzupełniające czynności audytowe niezbędne do uzyskania wystarczających i odpowiednich dowodów.
- 189 Zespół audytowy musi udokumentować swoją ocenę zewnętrznego materiału dowodowego uzasadnienia zaufania, zidentyfikowane

ograniczenia i proponowane czynności uzupełniające w zapisach z audytu i w raporcie z audytu.

- 190 Formalne ustalenie pełnego polegania, częściowego polegania lub braku polegania musi zostać dokonane przez CAB zgodnie z pkt 7.6–7.8 GP-03 i nie jest dokonywane przez zespół audytowy na podstawie postanowień niniejszego dokumentu.

B.10 Kompetencje, niezależność i outsourcing zespołu audytowego

B.10.1 Kompetencje zbiorowe

- 191 Zespół audytowy musi łącznie posiadać kompetencje odpowiednie do zakresu, obejmujące — stosownie do przypadku:
- System Certyfikacji PL Portfela EUDI i GP-03;
 - mające zastosowanie wymagania prawne, regulacyjne, normatywne i wymagania programu;
 - zarządzanie bezpieczeństwem informacji, cyberbezpieczeństwo i bezpieczeństwo sieci;
 - ocenę ryzyka i zarządzanie ryzykiem;
 - identyfikację elektroniczną, PID, Portfel EUDI i procesy uwierzytelniania;
 - kryptografię, PKI, komponenty bezpieczne i protokoły;
 - potwierdzanie tożsamości, zdalny onboarding, biometrię i zapobieganie oszustwom;
 - zasady audytu, metody, próbkowanie, ocenę dowodów i raportowanie;
 - technologie i procesy operacyjne objęte zakresem audytu.
- 192 Dokumenty WM-03-0x dotyczące poszczególnych kryteriów muszą wskazywać wszelkie dodatkowe kompetencje specjalistyczne wymagane do ich stosowania.

B.10.2 Kierownik zespołu audytowego i eksperci techniczni

- 193 Kierownik zespołu audytowego musi posiadać wystarczające doświadczenie audytowe i znajomość mających zastosowanie kryteriów, aby zarządzać audytem i konsolidować ustalenia.

- 194 Eksperci techniczni mogą doradzać audytorom w kwestiach specjalistycznych, lecz nie mogą działać jako jedyny oceniający zgodność ani podejmować decyzji certyfikacyjnej.

B.10.3 Outsourcing czynności audytowych

- 195 Czynności audytowe mogą być zlecane na zewnątrz wyłącznie w zakresie dozwolonym przez G-01, GP-03, G-05 i mające zastosowanie ramy normatywne.
- 196 CAB musi określić zakres outsourcingu, wymagania kompetencyjne, poufność, obowiązki sprawozdawcze i dostęp do zapisów.
- 197 CAB zachowuje odpowiedzialność za audyt, wnioski z oceny i decyzję certyfikacyjną.
- 198 CAB musi dokonać przeglądu i akceptacji wyników prac zleconych na zewnątrz przed ich wykorzystaniem jako dowodów w ocenie.

B.11 Proces audytu

- 199 *UWAGA: Audyt stanowi część etapu oceny GP-03. Opisany poniżej proces nie zastępuje etapu przygotowania i składania wniosku ani etapu certyfikacji zdefiniowanych w GP-03.*

B.11.1 Audyty początkowe i audyty ponownej oceny

- 200 *UWAGA: Audyty początkowe i audyty ponownej oceny powinny zwykle obejmować Etap 1 i Etap 2. Kolejność może zostać dostosowana, jeżeli jest to uzasadnione i dozwolone przez G-05 oraz plan audytu.*

B.11.2 Etap 1 — przegląd dokumentacji i gotowości

- 201 *UWAGA: Etap 1 ma na celu zrozumienie przedmiotu certyfikacji, potwierdzenie gotowości do audytu i zaplanowanie Etapu 2. Powinien obejmować, stosownie do przypadku:*

- zakres, ład organizacyjny i odpowiedzialności organizacyjne;
- architekturę, systemy, usługi, procesy, interfejsy i działania zlecone na zewnątrz;
- mające zastosowanie polityki, procedury i oświadczenia o praktykach;
- ocenę ryzyka, postępowanie z ryzykiem i właściwy rejestr ryzyka;

- *audyty wewnętrzne, przeglądy zarządzania, wcześniejsze ustalenia i zewnętrzne dowody uzasadnienia zaufania;*
- *dostępność zapisów, próbek, systemów, lokalizacji i personelu;*
- *obszary budzące wątpliwości oraz dodatkowe kompetencje lub czas wymagane na Etap 2.*

- 202 Wyniki Etapu 1 muszą zostać udokumentowane i wykorzystane do sfinalizowania planu Etapu 2.
- 203 Potencjalne niezgodności zidentyfikowane podczas Etapu 1 muszą być traktowane jako obszary budzące wątpliwości do czasu ich potwierdzenia wystarczającymi dowodami.

B.11.3 Etap 2 — wdrożenie i skuteczność operacyjna

- 204 Etap 2 musi obejmować zebranie obiektywnych dowodów na to, że mające zastosowanie wymagania są wdrożone i działają skutecznie.
- 205 *UWAGA: Etap 2 może obejmować przegląd dokumentacji, wywiady, obserwację, inspekcję, próbkowanie, przegląd transakcji, analizę logów i weryfikację techniczną.*
- 206 Etap 2 musi obejmować właściwe lokalizacje i środowiska operacyjne, chyba że uzyskano wystarczające równoważne dowody, a wykorzystanie technik zdalnych lub zewnętrznych dowodów uzasadnienia zaufania jest uzasadnione.

B.11.4 Audyty nadzoru i audyty specjalne

- 207 Audyty nadzoru i audyty specjalne mogą wykorzystywać ukierunkowaną, opartą na ryzyku sekwencję zamiast pełnego modelu Etapu 1 i Etapu 2. CAB musi jednak określić zakres, kryteria, metody, próbki, dowody i raportowanie wystarczające dla celu audytu.

B.11.5 Spotkania i komunikacja

- 208 Zespół audytowy musi przeprowadzić spotkanie otwierające lub inauguracyjne odpowiednie do audytu.
- 209 Istotne ustalenia mające wpływ na decyzję certyfikacyjną muszą być komunikowane bez zbędnej zwłoki, zgodnie z GP-03.
- 210 Spotkanie zamykające musi przedstawiać zakres audytu, metody, ograniczenia, ustalenia i dalsze kroki oraz musi zapewnić stronom audytowanym możliwość wyjaśnienia kwestii faktycznych.

B.12 Ocena ustaleń i zasady zaliczenia/niezaliczenia

B.12.1 Zastosowanie wymagań

- 211 Dla każdego wymagania ujętego w matrycy oceny zespół audytowy musi ustalić, czy ma ono zastosowanie do zatwierdzonego zakresu audytu.
- 212 Status zastosowania musi być jednym z następujących:
- Ma zastosowanie — wymaganie ma zastosowanie do zatwierdzonego zakresu audytu;
 - Nie ma zastosowania — wymaganie nie ma zastosowania do zatwierdzonego zakresu audytu, a uzasadnienie wyłączenia zostało udokumentowane i zaakceptowane.
- 213 Wymaganiu sklasyfikowanemu jako niemające zastosowania nie przypisuje się wyniku oceny zgodności.

B.12.2 Wyniki oceny na poziomie wymagań

- 214 Dla każdego mającego zastosowanie wymagania zespół audytowy musi przypisać jeden z wyników przedstawionych w Tabeli 3.

Tabela 3 Wyniki audytu

Wynik	Znaczenie
Zgodne	Wystarczające i odpowiednie obiektywne dowody wykazują spełnienie wyspecyfikowanego wymagania.
Duża niezgodność	Niespełnienie wyspecyfikowanego wymagania, które ma istotny wpływ na bezpieczeństwo i/lub istotny wpływ na zdolność przedmiotu certyfikacji do osiągnięcia zamierzonego rezultatu usługi lub procesu.
Mała niezgodność	Niespełnienie wyspecyfikowanego wymagania, które nie ma żadnego istotnego wpływu na bezpieczeństwo ani żadnego istotnego wpływu na zdolność przedmiotu certyfikacji do osiągnięcia zamierzonego rezultatu usługi lub procesu.
Nierozstrzygnięte — niewystarczające dowody	Wystarczające i odpowiednie dowody nie były dostępne, aby stwierdzić zgodność.

Wynik	Znaczenie
	Wynik ten nie może być traktowany jako zgodność i musi zostać rozstrzygnięty przed wydaniem pozytywnej rekomendacji z audytu w odniesieniu do mającego zastosowanie zakresu.

B.12.3 Spostrzeżenia

- 215 Zespół audytowy może odnotowywać pozytywne lub negatywne spostrzeżenia obok wyników oceny na poziomie wymagań.
- 216 *UWAGA: Spostrzeżenie to informacyjne ustalenie z audytu wskazujące ryzyko, słabość, dobrą praktykę lub pojawiający się problem, w przypadku którego dostępne dowody nie wykazują niespełnienia wyspecyfikowanego wymagania.*
- 217 Spostrzeżenie nie może zastępować wyniku oceny zgodności i samo w sobie nie może stanowić niespełnienia wymagania.

B.12.4 Związek z decyzją certyfikacyjną

- 218 Wyniki oceny i ustalenia z audytu muszą stanowić dane wejściowe do przeglądu i decyzji certyfikacyjnej przeprowadzanych zgodnie z GP-03 i G-05.
- 219 Zespół audytowy nie może wydawać decyzji certyfikacyjnej. Formalna decyzja certyfikacyjna musi zostać podjęta przez CAB zgodnie z mającym zastosowanie programem certyfikacji.

B.13 Raportowanie z audytu i powiązanie z raportem z oceny

B.13.1 Raport z audytu

- 220 Kierownik zespołu audytowego musi przekazać CAB raport z audytu o zawartości zgodnie z G-01, sekcja 6.3.
- 221 Raport z audytu musi zawierać wystarczający poziom szczegółowości, aby umożliwić niezależny przegląd audytu i jego wniosków.

B.13.2 Raport z oceny

- 222 GP-03 wymaga raportu z oceny obejmującego całość oceny. CAB może wykorzystać raport z audytu jako dane wejściowe albo wydać połączony raport z audytu i oceny, jeżeli audyt stanowi całość czynności oceny.
- 223 Raport z oceny musi zawierać ogólną ocenę zgodności z każdym mającym zastosowanie wymaganiem WZ-03, WP-03 i WM-03, ustalenie dotyczące polegania na zewnętrznych dowodach uzasadnienia zaufania oraz rekomendację dotyczącą decyzji certyfikacyjnej.
- 224 Jeżeli do raportu z oceny wnoszą wkład różne audyty, oceny lub raporty zewnętrzne, CAB musi zapewnić identyfikowalność od każdego wymagania do wykorzystanych dowodów i wniosków.

B.14 Działania korygujące i działania następcze

- 225 Dla każdej niezgodności wnioskodawca lub posiadacz certyfikatu musi przedstawić informacje odpowiednie do jej znaczenia, w tym korekcję, analizę przyczyny źródłowej, działanie korygujące, osobę odpowiedzialną, termin docelowy i dowody realizacji.
- 226 CAB musi ocenić adekwatność proponowanych działań korygujących i określić czynności weryfikacyjne wymagane do ich zamknięcia.
- 227 Duże niezgodności muszą zostać skorygowane, a ich zamknięcie zweryfikowane przed wydaniem pozytywnej rekomendacji certyfikacyjnej lub decyzji certyfikacyjnej.
- 228 Terminy dla małych niezgodności muszą być uzgadniane zgodnie z GP-03, G-05 i mającą zastosowanie procedurą CAB. Niniejsze ramy nie ustanawiają odrębnego sztywnego terminu.
- 229 Jeżeli niezgodność może dotyczyć wielu lokalizacji, systemów, procesów lub dostawców, działanie korygujące musi obejmować pełny zasięg systemowy i przyczynę leżącą u podstaw.
- 230 *UWAGA: Weryfikacja może być przeprowadzona poprzez przegląd dokumentów, wywiad, próbkowanie, obserwację, testowanie, dodatkowy audyt lub inną uzasadnioną metodę.*
- 231

B.15 Nadzór, ponowna ocena i audyty specjalne

- 232 Częstotliwość i zakres audytów muszą być zgodne z GP-03, w tym z corocznym nadzorem i ponowną oceną przed wygaśnięciem certyfikatu.
- 233 Planowanie audytu nadzoru musi uwzględniać istotne zmiany, incydenty, zaktualizowane dokumenty programu, informacje z rejestru ryzyka, informacje wywiadowcze, wyniki monitorowania zgodności, certyfikaty zewnętrzne i wcześniejsze ustalenia.
- 234 *UWAGA: Ponowna ocena może w udokumentowany sposób wykorzystywać akceptowalne dowody z czynności nadzoru i może ograniczać powielanie prac audytowych zgodnie z ustaleniem dotyczącym polegania na dowodach.*
- 235 Audyty specjalne muszą być inicjowane przez CAB w przypadku wystąpienia co najmniej jednego z następujących zdarzeń:
- istotne zmiany,
 - incydenty bezpieczeństwa,
 - skargi,
 - niewdrożenie działań korygujących lub inne informacje istotne dla ciągłej zgodności.
- 236 *UWAGA: Niniejsze ramy nie definiują samodzielnie decyzji o zawieszeniu, cofnięciu certyfikatu ani o ponownej certyfikacji; kwestie te reguluje GP-03, G-01 i G-05.*

B.16 Zapisy, poufność i kontrola jakości

- 237 CAB musi przechowywać plany audytów, zapisy dotyczące kompetencji, zapisy dowodowe, notatki, próbki, oceny polegania na dowodach, raporty, zapisy działań korygujących i zapisy przeglądów zgodnie z G-01 i G-05.
- 238 Dostęp do wrażliwych dowodów, w tym danych osobowych, architektury bezpieczeństwa, informacji kryptograficznych, podatności i informacji o incydentach, musi być ograniczony do osób upoważnionych, zgodnie z zasadą wiedzy koniecznej (need to know).
- 239 Dowody audytowe muszą być przekazywane, przechowywane i niszczone z zastosowaniem zabezpieczeń odpowiednich do ich wrażliwości.

- 240 CAB musi stosować mechanizmy przeglądu i kontroli jakości wystarczające do zapewnienia spójności ustaleń, klasyfikacji i raportowania pomiędzy zespołami audytowymi oraz dokumentami WM dotyczącymi poszczególnych kryteriów.
- 241 Kwestie interpretacyjne, których CAB nie może rozstrzygnąć, muszą być eskalowane zgodnie z zasadami ładu organizacyjnego programu certyfikacji.

Aneks C (normatywny) Minimalna zawartość planu audytu

242 Plan audytu musi zawierać co najmniej następujące elementy:

- identyfikację i rodzaj audytu;
- cele, zakres, granice i kryteria;
- zespół audytowy i role;
- terminy, czas trwania, lokalizacje i harmonogram czynności;
- ustalenia dotyczące Etapu 1 i Etapu 2, w stosownych przypadkach;
- metody, główne ścieżki audytu i planowane próbki;
- zewnętrzne dowody uzasadnienia zaufania i zamierzone podejście do polegania na nich;
- techniki zdalne, dostęp i rozwiązania w zakresie bezpieczeństwa informacji;
- ustalenia dotyczące spotkań, komunikacji i raportowania;
- znane ograniczenia, założenia i rozwiązania awaryjne.

Aneks D (normatywny) Minimalna zawartość zapisu dowodowego z audytu

243 Zapis dowodowy z audytu musi zawierać lub przywoływać co najmniej następujące elementy:

- wymaganie lub kryterium audytu;
- metodę audytu i ścieżkę audytu;
- przejrzone dokumenty i zapisy;
- osoby, z którymi przeprowadzono wywiady, i obserwowane procesy;
- zbadane systemy, lokalizacje i komponenty techniczne;
- populację próby, metodę doboru i wybrane elementy;
- zewnętrzne dowody uzasadnienia zaufania i wynik ustalenia polegania na nich;
- uzyskane obiektywne dowody;
- wniosek faktograficzny i wszelkie ograniczenia;
- odsyłacze do ustaleń i sekcji raportu.

Aneks E (normatywny) Matryca wyników oceny

Requirement	Applicability	Method	Evidence sample /	Reliance	Result	Finding reference
[ID]	Applicable / N/A	Document / interview / observation / sampling / test	[evidence and sample]	Full / Partial / None	C / Major NC / Minor NC / N/E / OBS	[reference]