

WM-02-01

**System Certyfikacji PL EUDI Wallet
Rozszerzenie metodyki FITCEM na
rozwiązanie EUDI Wallet**

WERSJA - 1.01

2026.07.21

/Załączony plik: WM-02-01_Test_plan_1.0.docx/

Sygnatura dokumentu	WM-02-01
Wersja	1.01
Status	Ostateczny
Data	21.07.2026
Typ dokumentu	Program certyfikacji — Metodyka
Ramy nadrzędne	GP-02, WP-02-01, WP-02-02, WP-02-03
Właściciel programu	Rzeczpospolita Polska / Minister Cyfryzacji
Przedmiot certyfikacji	Funkcjonalność cyberbezpieczeństwa EUDI Wallet Unit
Główni odbiorcy	Jednostki oceniające zgodność (CAB)
Pozostali odbiorcy	Dostawcy EUDI Wallet, dostawcy PID
Poziom uzasadnienia zaufania <potwierdzenie tożsamości CIR 2015/1502> lub <ocena, rozporządzenie UE 2019/881>	Wysoki (rozporządzenie UE 2019/881)
Dokumenty podrzędne	Brak

Historia zmian

Lp.	Zmiana	Wersja	Data
1.	Wersja oficjalna	1.0	2026-06-30
2.	Wydzielenie załącznika do osobnego pliku Zmiany edycyjne	1.01	2026-07-21

Spis treści

<u>1</u>	<u>ZAKRES.....</u>	<u>5</u>
<u>2</u>	<u>ODNIESIENIA</u>	<u>6</u>
2.1	Normy i specyfikacje techniczne	6
2.2	Dokumenty nadrzędne	6
<u>3</u>	<u>USZCZEGÓLOWIENIE ZADAŃ OCENY FITCEM</u>	<u>7</u>
3.1	Rozszerzenia zadań oceny FITCEM	7
3.2	Dodatkowe wymagania dla Dostawcy Portfela w fazie przygotowania i oceny	10
3.3	Ograniczenie oceny profilu ochrony.....	10
<u>4</u>	<u>RÓWNOWAŻNOŚĆ POZIOMU UZASADNIENIA ZAUFANIA.....</u>	<u>11</u>
4.1	Nakłady na ocenę	11
4.2	Wnioski.....	13
<u>5</u>	<u>BADANIA ZGODNOŚCI</u>	<u>14</u>
5.1	Wprowadzenie	14
5.2	Postanowienia ogólne	14
5.3	Dowody dostawcy (Vendor Evidence)	15
5.4	Ocena testowa (Test Evaluation)	15
5.5	Opis testu wraz z oczekiwanym wynikiem	16
5.6	Przygotowanie testu.....	17
5.7	Kroki testowe	17
5.8	Wynik testu.....	18
5.9	Ocena (pass/fail)	18
5.10	Werdykt testu	18
5.11	Dowody pomocnicze dla zachowań nieobserwowalnych.....	19
5.12	Ograniczenie zakresu.....	19
<u>6</u>	<u>ZAŁĄCZNIK A. ZESTAWIENIE DOWODÓW</u>	<u>20</u>

1 Zakres

- 1 W niniejszym dokumencie określono, w jaki sposób wymagania wyszczególnione w WP-02-02 wobec zdefiniowanego przedmiotu certyfikacji mogą być oceniane w sposób obiektywny i powtarzalny.
- 2 Dokument zawiera:
 - a) Uszczegółowienie metodyki oceny określonej w EN 17640:2022 + A1:2026 Ograniczona w czasie metodyka oceny cyberbezpieczeństwa produktów teleinformatycznych, w zakresie delegowanym przez normę na program certyfikacji. Obejmuje ono:
 - doprecyzowanie zakresu zadań oceny, które nie są bezpośrednio wskazane przez normę w odniesieniu do poziomu uzasadnienia zaufania „wysoki”, tj. przeglądu funkcjonalności zabezpieczeń (Review of Security Functionality) oraz testowania podatności (Vulnerability Testing),
 - dodatkowe wymagania dla Dostawcy Portfela mające zapewnić sprawny przebieg fazy przygotowania i oceny,
 - doprecyzowanie treści i miejsca dokumentu WP-02-02 w programie GP-02.
 - b) Uzasadnienie równoważności poziomu uzasadnienia zaufania „wysoki” w programie GP-02 z co najmniej AVA_VAN.3 w programie EUCC.
 - c) Indywidualna metodyka badań zgodności wraz z planem testów

2 Odniesienia

2.1 Normy i specyfikacje techniczne

- 3 ISO/IEC 17007 Ocena zgodności — Wytyczne dotyczące redagowania dokumentów normatywnych przeznaczonych do stosowania w ocenie zgodności
- 4 PN-EN ISO/IEC 17000:2020 Ocena zgodności — Terminologia i zasady ogólne
- 5 PN-EN ISO/IEC 15408:2023 (norma wieloczęściowa) Kryteria oceny zabezpieczeń informatycznych
- 6 PN-EN ISO/IEC 18045:2023 Kryteria oceny zabezpieczeń informatycznych — Metodyka oceny zabezpieczeń informatycznych
- 7 EN 17640:2022 + A1:2026 Ograniczona w czasie metodyka oceny cyberbezpieczeństwa produktów teleinformatycznych

2.2 Dokumenty nadrzędne

- 8 GP-02. Program certyfikacji cyberbezpieczeństwa
- 9 WP-02-01. Dekompozycja — wymagania bezpieczeństwa EUDI Wallet
- 10 WP-02-02. Profil ochrony FITCEM dla aplikacji — instancja EUDI Wallet
- 11 WP-02-03 EU CC Protection Profile for WSCA

3 Uszczegółowienie zadań oceny FITCEM

3.1 Rozszerzenia zadań oceny FITCEM

- 12 *UWAGA 1: Zakres oceny obejmuje oprogramowanie portfela dostarczane przez Dostawcę Portfela, w oparciu o założenia dotyczące platformy programowej i sprzętu.*
- 13 *UWAGA 2: Zakres zadań oceny został ujęty w GP-02 (określa on program certyfikacji, w ramach którego funkcjonuje FIT PP).*
- 14 Dostawca Portfela dostarcza następującą dokumentację rozwojową:
- a) Specyfikację funkcjonalną Instancji Portfela (Wallet Instance). Zawiera ona opis istotnego dla bezpieczeństwa zachowania funkcjonalnego aplikacji, w tym opis:
 - wszystkich interfejsów mających wpływ na bezpieczeństwo
 - parametrów interfejsów
 - zastosowanych mechanizmów kryptograficznych i powiązań
 - obsługi błędów oraz logiki walidacji stosowanej przez te interfejsy
 - b) Strukturę Instancji Portfela. Zawiera ona opis wewnętrznego projektu aplikacji, w tym dekompozycję TOE na komponenty oraz relacje między nimi. Opis projektu ma wspierać ocenę TOE poprzez wykazanie, w jaki sposób zaimplementowana funkcjonalność zabezpieczeń jest realizowana w systemie w zależności od platformy programowej.
 - c) Architekturę bezpieczeństwa Instancji Portfela. Zawiera ona opis:
 - domen bezpieczeństwa w ramach Instancji Portfela oraz ich separacji
 - procedur bezpiecznej inicjalizacji WI
 - ochrony WI przed manipulacją oraz obejściem funkcji zabezpieczeń
 - d) zestawienie komponentów oprogramowania TOE (Software Bill of Materials, SBOM)
 - e) Kod źródłowy aplikacji. Obejmuje on:

- kod źródłowy aplikacji, wraz z informacją o ścieżce kompilacji użytej do wygenerowania TOE (w celu weryfikacji sposobu integracji bibliotek zewnętrznych)
- wersję aplikacji z dezaktywowanymi mechanizmami zabezpieczeń
- wersję aplikacji umożliwiającą debugowanie
- kod wykorzystywany do kryptoanalizy bezpieczeństwa. Dla przejrzystości niektóre fragmenty mogą być przedstawione w formie pseudokodu

15 Wymieniona powyżej dokumentacja, dostarczana przez Dostawcę Portfela, została wskazana w GP-02 zgodnie z Załącznikiem I.

16 W fazie przygotowawczej realizowane są następujące działania, wskazane w GP-02 (rozdział 7 Procesy oceny i certyfikacji), z dodatkowymi nakładami:

a) Przegląd funkcjonalności zabezpieczeń

UWAGA 1: To zadanie oceny jest objęte programem (zob. GP-02, 7.1, tabela 4)

- Oceniający potwierdza, że funkcjonalności zabezpieczeń określone w zadaniu zabezpieczeń (Security Target) zostały precyzyjnie wyspecyfikowane i są zgodne z najlepszymi praktykami branżowymi.

UWAGA 2: W kolejnych krokach oceny potwierdzone jest, że te funkcjonalności zabezpieczeń zostały poprawnie zaimplementowane w produkcie.

b) Ocena zadania zabezpieczeń (Security Target, ST)

- Oceniający przeprowadza analizę odporności funkcji zabezpieczeń opisanych w zadaniu zabezpieczeń.

c) Przegląd dokumentacji rozwojowej

- Oceniający dokonuje przeglądu dokumentacji dostarczonej przez dewelopera.

UWAGA 3: CAB-ITSEF może wymagać wsparcia ze strony dewelopera przy przeglądzie kodu źródłowego, aby przegląd ten był efektywny.

UWAGA 4: analiza ta obejmuje również, w razie potrzeby, ocenę protokołów implementujących interfejsy aplikacji mobilnej (i ewentualnie innych interfejsów). Na podstawie tej analizy opracowywany jest plan badań zgodności i testów penetracyjnych.

17

W fazie oceny:

a) Ocena instalacji TOE

b) Badania zgodności

— *UWAGA 6: to zadanie testowe opiera się na testach obejmujących analizę kodu źródłowego (przegląd kodu źródłowego) oraz obserwację zachowania aplikacji. Dodatkowo oceniający będą korzystać z wyników swojej analizy dokumentacji dostarczonej przez dewelopera.*

— Oceniający weryfikuje, czy implementacja aplikacji spełnia wymagania bezpieczeństwa określone w WP-02-02.

c) Przegląd podatności wraz z testowaniem podatności

— *UWAGA 7: To zadanie przeglądowe opiera się na analizie podatności zgodnie ze źródłami odzwierciedlającymi aktualny stan wiedzy. Danymi wejściowymi dla tego kroku są dokumentacja rozwojowa wymieniona w GP-02, załączniki C-D, oraz raport podatności zawarty w SBOM.*

— Zadanie oceny obejmuje wszystkie jednostki pracy (Work Units) mające zastosowanie dla poziomu uzasadnienia zaufania „istotny” (substantial).

d) Testy penetracyjne

e) Analiza kryptograficzna (rozszerzona)

f) Ocena złożonego TOE (Composite TOE)

18

W technicznym raporcie z oceny (Evaluation Technical Report) Ewaluator opisuje założenia techniczne oraz środowisko testowe wykorzystane do obserwacji zachowania aplikacji.

19 *PRZYKŁAD: Dostawca Portfela wskazuje, czy wykorzystano zdegradowane wersje aplikacji lub czy opracowano dedykowane narzędzia.*

3.2 **Dodatkowe wymagania dla Dostawcy Portfela w fazie przygotowania i oceny**

20 Od Dostawcy Portfela wymagane są następujące ustalenia:

- a) **Dostarczenie kodu źródłowego Instancji Portfela,**
W przypadku, gdy kod źródłowy jest zaciemniony (obfuskowany), Dostawca Portfela dostarcza plik wygenerowany po kompilacji/transformacji, umożliwiający prześledzenie powiązań między oryginalnymi klasami, metodami i zmiennymi a wynikiem obfuskacji.
- b) W przypadku, gdy WI korzysta z infrastruktury zaplecza (back-end) Dostawcy Portfela, której nie można odtworzyć w siedzibie CAB-ITSEF, **Dostawca Portfela udziela oceniającym dostępu do niezbędnych elementów środowiska deweloperskiego** oraz zobowiązuje się nie wprowadzać żadnych zmian w ich konfiguracji przez cały okres fazy oceny, a także zapewnić unikalny identyfikator tego środowiska.
- c) **Dostawca Portfela zapewnia wszystkie konta niezbędne do właściwego korzystania z aplikacji** (administracyjne, użytkowników itp.) przed rozpoczęciem fazy oceny.
- d) **Dostawca Portfela zapewnia cały sprzęt niezbędny do oceny WI**, w tym przykładowe urządzenia końcowe, dowody osobiste do użycia z Instancją Portfela itp.

3.3 **Ograniczenie oceny profilu ochrony**

21 Mając na uwadze, że profil ochrony (zidentyfikowany jako część Systemu Certyfikacji PL EUDI Wallet, WP-02-02) odpowiada określonej celowi programu, tj. zawiera wymagania bezpieczeństwa dla aplikacji mobilnej, GP-02 nie nakłada żadnych wymagań dotyczących certyfikacji tego profilu ochrony.

4 Równoważność poziomu uzasadnienia zaufania

4.1 Nakłady na ocenę

- 22 *UWAGA: Ze względu na specyficzną treść analizy, niniejszy rozdział zawiera uzasadnienie dla poziomu uzasadnienia zaufania „wysoki”, zgodnego z Aktem o cyberbezpieczeństwie w odniesieniu do metodyki oceny FITCEM. W związku z tym nie zawiera on żadnych wymagań.*
- 23 Przeanalizujmy nakłady na ocenę wymagane do osiągnięcia poziomu uzasadnienia zaufania „wysoki” zgodnie z CSA. Wykażemy równoważność z co najmniej AVA_VAN.3, który stanowi minimalne kryterium dla poziomu uzasadnienia zaufania „wysoki” w programie EUCC.
- 24 Wyniki dyskusji na temat równoważności metodyk oceny FITCEM i EUCC przedstawiono w Tabeli 1.

Tabela 1 Zadania oceny i działania oceniające

Zadania oceny	Równoważność FITCEM dla poziomu uzasadnienia zaufania „wysoki”	Równoważność EUCC dla poziomu uzasadnienia zaufania „wysoki” na podstawie zależności AVA_VAN.3	Uwagi dodatkowe
Kontrola kompletności	Wymagane	Brak w EUCC konkretnego komponentu uzasadnienia zaufania	Kontrola kompletności opiera się na publicznie dostępnych informacjach o produkcie (karty katalogowe, informacje na stronie internetowej itp.)
Przegląd funkcjonalności zabezpieczeń	Wymagane	ADV_FSP.4 Kompletna specyfikacja funkcjonalna	Wymagany w GP-02 uproszczony dokument funkcjonalności bezpieczeństwa, zbliżony do dokumentu wymaganego w EUCC w klasie ADV.
Ocena zadania zabezpieczeń	Wymagane	Pośrednio implikowane	Równoważne klasie ASE

Zadania oceny	Równoważność FITCEM dla poziomu uzasadnienia zaufania „wysoki”	Równoważność EUCC dla poziomu uzasadnienia zaufania „wysoki” na podstawie zależności AVA_VAN.3	Uwagi dodatkowe
Dokumentacja rozwojowa	Wymagane	ADV_ARC.1 Opis architektury bezpieczeństwa ADV_TDS.3 Podstawowy projekt modułowy	Wymagane w GP-02 uproszczone dokumenty architektury rozwiązania, zbliżone do dokumentów wymaganych w EUCC.
Ocena instalacji TOE	Wymagane	AGD_PRE.1 Procedury przygotowawcze AGD_OPE.1 Przewodnik użytkownika dotyczący eksploatacji	Część przygotowawcza jest równoważna FITCEM Przewodnik użytkownika dotyczący eksploatacji jest równoważny Przewodnikowi bezpiecznego użytkownika (Secure User Guide) w FITCEM
Badania zgodności	Wymagane	ATE_IND.1 (Testy niezależne)	FITCEM obejmuje więcej niż ATE_DPT.1 i ATE_IND.1
Testy penetracyjne	Wymagane	AVA_VAN.3 Ukierunkowana analiza podatności	Metoda hipotezy wady (Flaw Hypothesis Methodology; obowiązkowa dla AVA_VAN.3 również w CC)
Rozszerzona analiza kryptograficzna	Wymagane	ADV_IMP.1 Reprezentacja implementacji TSF	Rozszerzenie wymagania prezentacji kodu źródłowego – równoważne ADV_IMP.1

4.2 Wnioski

- 25 Analizując równoważność obu metodyk w odniesieniu do poziomu uzasadnienia zaufania „wysoki”, należy uwzględnić dwa elementy składające się na ten poziom (zob. CSA, art. 52 ust. 7):
- a) *[produkt ICT] spełnia odpowiednie wymagania bezpieczeństwa, w tym funkcjonalności zabezpieczeń, oraz*
- b) *[produkt ICT] został oceniony na poziomie mającym na celu zminimalizowanie ryzyka cyberataków odzwierciedlających aktualny stan wiedzy, przeprowadzanych przez podmioty dysponujące znacznymi umiejętnościami i zasobami.*
- 26 FITCEM spełnia oba wymienione wyżej elementy.
- 27 Ad a) — weryfikacja zgodności z wymaganiami bezpieczeństwa jest pokryta co najmniej przez działania oceniające „Dokumentacja rozwojowa” i „Badania zgodności” w FITCEM.
- 28 Ad b) — nakłady na ocenę dotyczące odpowiedniego potencjału ataku oraz konieczności przeprowadzenia testów penetracyjnych są pokryte co najmniej przez działania oceniające „Przegląd podatności”, „Testowanie podatności” i „Testy penetracyjne”. Ponieważ FITCEM uwzględnia podejście oparte na hipotezach wad, obowiązkowe dla AVA_VAN.3 w Common Criteria, równoważność można uznać za wykazaną.
- 29 Należy zauważyć, że zastosowanie w ocenie wyłącznie AVA_VAN.3, bez jego zależności, nie jest wystarczające do osiągnięcia poziomu uzasadnienia zaufania „wysoki” zgodnie z definicją z CSA. W świetle elementu a) definicji jest jasne, że w przypadku oceny opartej na CC należy uwzględnić co najmniej pozostałe rodziny klasy ATE. Aby pokryć obsługę podatności, należy dodać co najmniej ALC_FLR.
- 30 Wykazano zatem, że FITCEM może być stosowany do każdej oceny cyberbezpieczeństwa wymagającej poziomu uzasadnienia zaufania „wysoki” zgodnie z definicją CSA. Biorąc pod uwagę poziom potencjału ataku, FITCEM w części dotyczącej uzasadnienia zaufania można porównać z komponentem AVA_VAN.3 zdefiniowanym w Common Criteria, o ile wdrożone zostaną wszystkie działania oceniające FITCEM dedykowane poziomowi uzasadnienia zaufania „wysoki” (obowiązkowe.).

5 Badania zgodności

5.1 Wprowadzenie

- 31 Badania zgodności z wymaganiami są ustrukturyzowane zgodnie z opisem w [FITCEM] 6.7.4.2 i obejmują następujące elementy:
- a) opis testu wraz z oczekiwanym wynikiem, przygotowanie testu oraz kroki testowe;
 - b) wynik testu;
 - c) ocenę (pass/fail).
- 32 Plan testów zapewnia, że dla każdego wymagania opracowany zostanie co najmniej jeden test zgodności,
- 33 *UWAGA 1: Pojedynczy przypadek testu zgodności może dostarczać dowodów dla wielu wymagań.*

5.2 Postanowienia ogólne

- 34 *UWAGA 1: Metodyka ogranicza się do badań zgodności TOE z wymaganiami FITCEM PP. Zapewnia wspólną i powtarzalną strukturę definiowania dowodów dostawcy, procedur testowych i werdyktów.*
- 35 *UWAGA 2: Metodyka opiera się na tabeli oceny dla każdego wymagania FITCEM PP. Każda tabela definiuje dowody dostawcy (Vendor Evidence, VE), ocenę testową (Test Evaluation, TE) oraz werdykt testu (Test Verdict).*
- 36 **CTM-01-GE-01**
- 37 Dla każdego wymagania FITCEM PP tabela oceny definiuje dowody dostawcy (VE) oraz ocenę testową (TE).
- 38 *UWAGA: VE określa dowody, które ma dostarczyć dostawca. TE określa czynność testową, którą ma wykonać tester.*
- 39 **CTM-01-GE-02**
- 40 Tester stosuje metodykę do kategorii wymagań FITCEM PP objętych zestawem testów, w tym: uwierzytelnianie i autoryzacja, rejestrowanie zdarzeń, usługi, magazyn lokalny, sieć i interfejsy, przewodnik bezpiecznego użytkowania, dokumentacja bezpieczeństwa, dodatkowe środki bezpieczeństwa oraz kryptografia.

41 **CTM-01-GE-03**

42 Ocena jest przeprowadzana wyłącznie dla ocenianej wersji TOE,
kompilacji, konfiguracji, zestawu platform i środowiska eksploatacji.

43 *UWAGA: Metodyka jest zgodna ze strukturą badań zgodności EN 17640
poprzez rozróżnienie oczekiwanego wyniku testu, przygotowania testu,
kroków testowych, rzeczywistego wyniku testu oraz oceny pass/fail.*

5.3 Dowody dostawcy (Vendor Evidence)

44 **CTM-01-VE-01**

45 Dostawca dostarcza dowody wystarczające do identyfikacji TOE, jego
ocenianej konfiguracji oraz zachowania istotnego dla danego wymagania.

46 **CTM-01-VE-02**

47 Dowody dostawcy zapewniają identyfikowalność od wymagania FITCEM
PP do zadeklarowanego projektu, konfiguracji, implementacji i
konfiguracji testowej.

48 **CTM-01-VE-03**

49 W przypadku gdy wymagane zachowanie nie może być w pełni
zaobserwowane poprzez interfejs użytkownika TOE lub zwykłe interfejsy
zewnętrzne, dostawca dostarcza kontrolowane dowody pomocnicze
wystarczające do przeprowadzenia oceny.

50 *UWAGA: Dowody takie mogą obejmować SUG, specyfikację funkcjonalną,
dowody konfiguracji, artefakty protokołów, logi, wyjście testowego punktu
końcowego, wyjście upręży testowej, mapowanie API, tabele decyzyjne,
diagramy stanów, ograniczone fragmenty kodu źródłowego lub logi testów
dostawcy.*

51 **CTM-01-VE-04**

52 Dowody są specyficzne dla ocenianej wersji i konfiguracji TOE. Dowody
ogólne, nieaktualne lub niepowiązane nie są wystarczające do werdyktu
PASS.

5.4 Ocena testowa (Test Evaluation)

53 **CTM-01-TEG-01**

54 Każde TE definiuje, w jaki sposób tester weryfikuje spełnienie
wymagania.

55 **CTM-01-TEG-02**

56 Można zdefiniować więcej niż jedno TE, jeżeli wymaganie obejmuje
niezależne zachowania, których nie można ocenić w ramach jednego
spójnego testu.

57 **CTM-01-TEG-03**

58 Każde TE wskazuje ścieżkę testową wykorzystywaną przez testera.
Ścieżka może opierać się na zachowaniu interfejsu użytkownika,
artefaktach protokołów, generowanych obiektach, logach, testowych
punktach końcowych, wyjściu diagnostycznym, obserwacji wspieranej
przez platformę lub kontrolowanych dowodach pomocniczych.

59 **CTM-01-TEG-04**

60 Każde TE zawiera następujące pięć elementów: opis testu wraz z
oczekiwanym wynikiem; przygotowanie testu; kroki testowe; wynik
testu; ocenę (pass/fail).

61 *UWAGA: Oczekiwany wynik testu określa oczekiwane zachowanie zgodne.
Wynik testu rejestruje rzeczywiste zaobserwowane lub w inny sposób
zweryfikowane zachowanie.*

5.5 Opis testu wraz z oczekiwanym wynikiem

62 **CTM-01-TE-DESC-01**

63 Opis testu wskazuje zachowanie, decyzję, mechanizm kontrolny, interfejs,
artefakt lub stan podlegający weryfikacji.

64 **CTM-01-TE-DESC-02**

65 Oczekiwany wynik testu określa oczekiwany zgodny rezultat w sposób
umożliwiający porównanie z rzeczywistym wynikiem.

66 *UWAGA: Oczekiwanie może odnosić się do pomyślnego wykonania, odmowy,
zablokowania, maskowania, odrzucenia, bezpiecznej awarii, ponownego
uwierzytelnienia, potwierdzenia, chronionego przechowywania, stanu
zaszyfrowanego, obsługi integralności, powiązania sesji, świeżości lub
innego rezultatu specyficznego dla wymagania.*

5.6 Przygotowanie testu

67 **CTM-01-TE-PREP-01**

68 Przygotowanie testu wskazuje konfigurację TOE, konta testowe, dane testowe, platformę, testowy punkt końcowy, wsparcie zaplecza (backend), środowisko testowe WSCA/WSCD lub inne warunki wstępne niezbędne do wykonania testu.

69 **CTM-01-TE-PREP-02**

70 Przygotowanie wskazuje próbkę wybraną do testu, jeżeli wymaganie obejmuje wiele funkcji, klas danych, przepływów, platform, partnerów, klas kluczy lub stanów cyklu życia.

5.7 Kroki testowe

71 **CTM-01-TE-STEP-01**

72 Kroki testowe opisują czynności wykonywane przez testera w powtarzalnej sekwencji.

73 **CTM-01-TE-STEP-02**

74 Tester rejestruje wersję TOE, platformę, ocenianą konfigurację, wybraną próbkę, metodę obserwacji oraz źródło dowodów.

75 **CTM-01-TE-STEP-03**

76 Jeżeli zachowanie jest bezpośrednio obserwowalne, tester wykonuje odpowiedni przepływ TOE i obserwuje wynik.

77 **CTM-01-TE-STEP-04**

78 Jeżeli zachowanie nie jest bezpośrednio obserwowalne, tester dokonuje przeglądu kontrolowanych dowodów pomocniczych i, o ile to możliwe, koreluje je z obserwowalnym zachowaniem lub artefaktem TOE.

79 *UWAGA: Dotyczy to piaskownicy (sandboxing), ograniczeń IPC, obsługi danych szczytkowych, chronionego przechowywania, wykorzystania magazynu kluczy wspieranego sprzętowo, konfiguracji kryptograficznej, walidacji certyfikatów, powiązania sesji, świeżości oraz wewnętrznej logiki decyzyjnej.*

5.8 Wynik testu

80 CTM-01-TE-RES-01

81 Wynik testu rejestruje rzeczywiste zachowanie zaobserwowane lub w inny sposób zweryfikowane przez testera.

82 CTM-01-TE-RES-02

83 Wynik testu wskazuje, czy testowane zachowanie było zgodne, niezgodne, niespójne, niejednoznaczne, nieudowodnione czy nie ma zastosowania.

5.9 Ocena (pass/fail)

84 CTM-01-TE-ASS-01

85 Ocena definiuje jednoznaczne warunki PASS i FAIL dla danego TE.

86 CTM-01-TE-ASS-02

87 TE otrzymuje wynik PASS wyłącznie wtedy, gdy dowody oraz zaobserwowane lub w inny sposób zweryfikowane zachowanie wykazują spełnienie wymagania dla ocenianej konfiguracji.

88 CTM-01-TE-ASS-03

89 TE otrzymuje wynik FAIL, jeżeli wymagane zachowanie nie występuje, jest sprzeczne z obserwacją, nie daje się powiązać z ocenianym TOE, zostało wykonane w nieprawidłowych warunkach lub nie zostało wystarczająco udokumentowane.

90 CTM-01-TE-ASS-04

91 Jeżeli test nie może zostać wykonany z powodu braku lub niewystarczających dowodów dostawcy, TE otrzymuje wynik FAIL, chyba że program wyraźnie dopuszcza uzasadniony wynik „nie ma zastosowania”.

5.10 Werdykt testu

92 CTM-01-TV-01

93 Werdykt testu dla wymagania to PASS wtedy i tylko wtedy, gdy wszystkie wymagane TE dla tego wymagania uzyskają wynik PASS.

94 **CTM-01-TV-02**

95 Werdykt testu to FAIL, jeżeli którekolwiek TE zakończy się niepowodzeniem lub jeżeli dowody VE są niewystarczające do wykonania lub innej weryfikacji wymaganych testów.

5.11 Dowody pomocnicze dla zachowań nieobserwowalnych

96 **CTM-01-NUI-01**

97 Jeżeli wymaganie nie może być zweryfikowane bezpośrednio poprzez interfejs użytkownika lub zwykły interfejs zewnętrzny, tester korzysta z kontrolowanej ścieżki dowodów pomocniczych.

98 **CTM-01-NUI-02**

99 Ścieżka dowodów pomocniczych ogranicza się do dowodów niezbędnych do wydania werdyktu zgodności.

100 **CTM-01-NUI-03**

101 Wykorzystanie dokumentacji, konfiguracji lub ograniczonych dowodów z kodu źródłowego nie jest traktowane jako pełny przegląd kodu źródłowego, inżynieria wsteczna, testowanie podatności ani analiza kryptograficzna.

5.12 Ograniczenie zakresu

102 *UWAGA: Badania zgodności weryfikują zadeklarowane zachowanie, integrację, wywoływanie, mechanizmy bramkujące, egzekwowanie decyzji, bezpieczną awarię oraz rezultaty obserwowalne lub udokumentowane.*

103 *UWAGA: Badania zgodności same w sobie nie dowodzą siły kryptograficznej, odporności na exploity, odporności na ataki bocznokanałowe, odporności na analizę śledczą pamięci, odporności na obejście root/jailbreak, solidności protokołów ani poprawności bezpiecznej implementacji. Jeżeli takie właściwości są istotne, ocenia się je w ramach odrębnych działań: analizy podatności, analizy kryptograficznej, przeglądu kodu źródłowego, bezpieczeństwa platformy lub testów penetracyjnych.*

6 Załącznik A. Zestawienie dowodów

Lp.	Charakterystyka dokumentów i zakres pokrycia	Odniesienie do GP-02
1	Zadanie zabezpieczeń (Security Target)	GP-02/Annex A PL EUDI Wallet Certification System Template for Wallet Instance Security Target
2	Przewodnik bezpiecznego użytkowania (Secure User Guide)	GP-02/Annex B PL EUDI Wallet Certification System Requirements for the evaluation of Secure User Guide
3	Dokumentacja rozwojowa obejmująca: • specyfikację funkcjonalną, • projekt TOE, • specyfikację architektury bezpieczeństwa, • zestawienie komponentów oprogramowania (SBOM)	GP-02/Annex C PL EUDI Wallet Certification System Requirements for the evaluation of functional specification and TOE design
4	Kod źródłowy wykorzystywany do kryptoanalizy bezpieczeństwa, opcjonalnie uzupełniony pseudokodem	GP-02/Annex D PL EUDI Wallet Certification System Requirements for the evaluation of cryptographic mechanisms
5	Kod źródłowy	GP-02 System Certyfikacji PL EUDI Wallet