

WM-02-02

System Certyfikacji PL Portfela EUDI
Adaptacja oceny opartej na ISO/IEC CEM
dla komponentu WSCA

WERSJA - 1.01

2026.07.23

Oznaczenie dokumentu	WM-02-02
Wersja	1.01
Status	Final
Data	23.07.2026
Rodzaj 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	WSCA
Odbiorcy pierwotni	Jednostki oceniające zgodność (CAB)
Odbiorcy wtórni	Dostawcy Portfela EUDI
<ocena, rozporządzenie (UE) 2019/881>	Wysoki
Dokumenty podrzędne	Brak

Historia zmian

Nr.	Zmiana	Wersja	Data
1.	Tłumaczenie wersji angielskiej	1.0	2026-07-08
2.	Drobne zmiany w sekcji 4 uwzględniające uwagi agencji ENISA Zmiany edycyjne	1.01	2026-07-23

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
2.3	Dokumenty stanowiące podstawę prawną	6
<u>3</u>	<u>DERYWACJA OPARTA NA ISO/IEC 15408-4 DLA KOMPONENTU</u>	
<u>ALC DVS.1.....</u>	<u>.....</u>	<u>7</u>
<u>4</u>	<u>METODYKA PRZEPROWADZANIA OCENY PODATNOŚCI NA POZIOMIE</u>	
<u>AVA VAN.5.....</u>	<u>.....</u>	<u>8</u>
<u>5</u>	<u>BADANIA ZGODNOŚCI</u>	<u>10</u>

1 Zakres

- 1 W niniejszym dokumencie określono dodatkowe wymagania dotyczące stosowania [CC] i [CEM] przy ocenie WSCA. Wymagania te dotyczą:
- ponownego wykorzystania materiału dowodowego uzasadnienia zaufania z powiązanych czynności oceny w ramach programu certyfikacji GP-03,
 - metodyki przeprowadzania oceny podatności dla komponentu AVA_VAN.5 w świetle nowo opublikowanej normy EN ISO/IEC 18045:2026.

2 Odniesienia

2.1 Normy i specyfikacje techniczne

- 2 [17007] ISO/IEC 17007 Ocena zgodności — Wytyczne dotyczące redagowania dokumentów normatywnych przeznaczonych do stosowania w ocenie zgodności
- 3 [17000] PN-EN ISO/IEC 17000:2020 Ocena zgodności — Terminologia i zasady ogólne
- 4 [CC] PN-EN ISO/IEC 15408:2023 (wieloczęściowa) Kryteria oceny zabezpieczeń informatycznych
- 5 [CEM] PN-EN ISO/IEC 18045:2023 Kryteria oceny zabezpieczeń informatycznych — Metodyka oceny zabezpieczeń informatycznych

2.2 Dokumenty nadrzędne

- 6 GP-02. Program certyfikacji cyberbezpieczeństwa
- 7 WP-02-01. Decomposition - EUDI Wallet security requirements
- 8 WP-02-02. FITCEM protection profile for the application - EUDI Wallet instance
- 9 WP-02-03 EU CC Protection Profile for WSCA

2.3 Dokumenty stanowiące podstawę prawną

- 10 [CIR 2024/2979] Rozporządzenie wykonawcze Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. w sprawie integralności i podstawowych funkcjonalności europejskich portfeli tożsamości cyfrowej.

3 Derywacja oparta na ISO/IEC 15408-4 dla komponentu ALC_DVS.1

- 11 Wszystkie subakcje oceny komponentu ALC_DVS.1 (tj. wymagania zawarte w [CCpart3] oraz wynikający z nich materiał dowodowy uzasadnienia zaufania określone w [CEM]) muszą zostać zastąpione ramami audytu GP-03 opisanymi w dokumentach serii WZ-03, WP-03 i WM-03, w zakresie odnoszącym się do bezpieczeństwa procesu rozwoju u dostawcy Portfela EUDI.

4 Metodyka przeprowadzania oceny podatności na poziomie AVA_VAN.5

- 12 *UWAGA 1: Dodatkowe wymagania zawarte w niniejszym rozdziale zostały wywiedzione z nowej wersji normy EN ISO/IEC 18045:2026, która koryguje oczywiste pominięcia występujące w wersji z 2022 r.*
- 13 Ocena podatności komponentu WSCA musi być przeprowadzana zgodnie z czynnością oceny AVA_VAN.5 zdefiniowaną w [CC] i [CEM].
- 14 Przede wszystkim, analiza metodyczna narzucona przez [CC] i [CEM] musi koncentrować się na weryfikacji, czy oceniany przedmiot oceny (TOE), którym jest komponent WSCA, spełnia funkcjonalne wymagania bezpieczeństwa zdefiniowane w specyfikacji zabezpieczeń (Security Target) WSCA.
- 15 *UWAGA 2: Celem analizy jest weryfikacja zgodności z wymaganiami dotyczącymi funkcjonalności bezpieczeństwa WSCA opisanymi w art. 5 [CIR 2024/2979].*
- 16 Jako wstępny krok analizy ewaluator musi określić aktywa krytyczne, zgodnie z definicją zawartą w [CIR 2024/2979], w zakresie ocenianego WSCA, poprzez przeprowadzenie analizy przepływu zasobów oraz cyklu życia.
- 17 Podczas badania publicznie dostępnych źródeł informacji w celu identyfikacji potencjalnych podatności ewaluator musi traktować jako podmiot, w którym podatność może wystąpić, zarówno TOE oraz konkretne produkty IT w środowisku, od których TOE zależy.
- 18 *UWAGA 3: Wszystkie one mogą mieć wpływ na funkcjonalność bezpieczeństwa TOE i jego bezpieczne działanie.*
- 19 W przeprowadzanej analizie metodycznej każda potencjalna podatność wymieniona w [CEM], podrozdział 17.2.5.6.1 Work Unit AVA_VAN.5-4 (tj. potencjalne podatności właściwe dla typu ocenianego TOE: obchodzenie zabezpieczeń, manipulacja, ataki bezpośrednie, monitorowanie, niewłaściwe użycie), musi zostać rozważona w celu poszukiwania możliwych sposobów przełamania ochrony funkcjonalności bezpieczeństwa TOE (TSF) i podważenia TSF.
- 20 Wszystkie zidentyfikowane potencjalne podatności, które są kandydatami do testowania i mają zastosowanie do TOE w jego środowisku operacyjnym, muszą zostać odnotowane przez ewaluatora w technicznym raporcie z oceny (Evaluation Technical Report, ETR).
- 21 Niemniej jednak w ETR można wskazać i wyjaśnić, że dalsze rozpatrywanie danej potencjalnej podatności nie jest wymagane.

- 22 *PRZYKŁAD: Taka sytuacja może mieć miejsce, gdy ewaluator stwierdzi, że środki w środowisku operacyjnym, informatyczne lub pozainformatyczne, uniemożliwiają wykorzystanie potencjalnej podatności w tym środowisku operacyjnym. Ewaluator musi odnotować wszelkie powody wyłączenia potencjalnych podatności z dalszego rozpatrywania.*
- 23 Jeżeli w ocenianym WSCA zostanie wykryta podatność możliwa do wykorzystania, ewaluator musi wskazać w ETR, które z wymagań dotyczących WSCA opisanych w art. 5 [CIR 2024/2979] zostało naruszone.

5 **Badania zgodności**

- 24 Dla każdego wymagania musi istnieć co najmniej jeden test zgodności; dla jednego wymagania może istnieć więcej niż jeden test.
- 25 *Uwaga 1: Pojedynczy przypadek oceny może dostarczać dowodów dla wielu wymagań.*
- 26 *Uwaga 2: Testy zgodności odnoszą się do klasy uzasadnienia zaufania ATE [CC part 3]*
- 27 Testy zgodności względem wymagań muszą mieć strukturę opisaną poniżej:
1. Odniesienie testu: identyfikuje dokładne identyfikatory wymagania (wymagań) oraz powiązane klauzule objęte danym przypadkiem oceny, tak aby zakres i identyfikowalność były jednoznaczne.
 2. Cel testu: określa konkretną właściwość bezpieczeństwa lub zdolność, która musi zostać zweryfikowana.
 3. Przygotowanie testu: opisuje środowisko testowe, warunki wstępne, narzędzia i konfigurację produktu wymagane przed wykonaniem testu.
 4. Czynności testowe: wymienia konkretne kroki przeglądu, testowania i obserwacji do wykonania, pokazujące, w jaki sposób implementacja ogranicza odwzorowane zagrożenia dla zadeklarowanej konfiguracji i poziomu ryzyka.
 5. Werdykt testu: definiuje kryteria zaliczenia/niezaliczenia (pass/fail) oraz sposób interpretacji wyników.
 6. Dowody testu: gromadzi wszystkie artefakty pomocnicze niezbędne do wykazania, że wymaganie zostało ocenione i spełnione.