

WM-03-03

System Certyfikacji PL Portfela EUDI

Ramy audytu cyberbezpieczeństwa

dla dostawców Portfela EUDI

WERSJA – 1.01

2026.07.21

/Załączony plik: WM-03-03_Annex A.docx/

Oznaczenie dokumentu	WM-03-03 Ramy audytu cyberbezpieczeństwa dla dostawców Portfela EUDI
Wersja	V1.01
Status	FINAL
Data	2026-07-21
Rodzaj dokumentu	Metody i techniki oceny – ogólne ramy audytu cyberbezpieczeństwa
Ramy nadrzędne	GP-03, seria WZ-03, seria WP-03
Właściciel programu	Rzeczpospolita Polska / Minister Cyfryzacji
Program certyfikacji	GP-03 Program certyfikacji eID
Odbiorcy pierwotni	Jednostki oceniające zgodność (CAB), kierownicy zespołów audytowych, auditorzy i eksperci techniczni
Zastosowanie	Audyty przeprowadzane w ramach fazy oceny zgodnie z GP-03
Dokumenty podrzędne	brak

Historia zmian

Nr.	Zmiana	Wersja	Data
1.	Tłumaczenie wersji angielskiej	1.0	2026-06-30
2.	Wydzielenie załącznika do osobnego pliku; Poprawki redakcyjne	1.01	2026-07-21

Cel

- 1 Niniejszy dokument stanowi uzupełnienie dokumentu GP-03/Annex B „Ogólne ramy audytu cyberbezpieczeństwa dla Programu certyfikacji eID”, właściwe dla poszczególnych kryteriów.
- 2 Metodyka audytu na potrzeby oceny dostawców Portfela EUDI została określona w GP-03/Annex B. W szczególności, GP-03/Annex B ustanawia wspólne zasady dotyczące planowania audytu, zakresu audytu, czasu audytu, metod i technik audytu, dowodów z audytu, doboru próby, wykorzystania zewnętrznych dowodów uzasadniających zaufanie, kompetencji zespołu audytowego, procesu audytu, oceny ustaleń, zasad zaliczenia/niezaliczenia (pass/fail), raportowania, działań korygujących oraz działań poaudytowych.
- 3 Niniejszy dokument nie powinien być stosowany jako samodzielny dokument metodyki audytu. Powinien on być stosowany wyłącznie łącznie z GP-03/Annex B, GP-03, G-01, G-05 oraz mającymi zastosowanie dokumentami WZ-03 i WP-03.
- 4 Tabela zamieszczona w załączniku do niniejszego dokumentu uzupełnia GP-03/Annex B, określając metody audytu na poziomie poszczególnych wymagań na potrzeby oceny dostawców Portfela EUDI. Dla każdego wymagania w tabeli wskazano wymaganie źródłowe, właściwy dokument źródłowy WZ/WP oraz minimalne czynności oceny CAB, które należy wykonać podczas etapu 1 i etapu 2.
- 5 Kolumna „Metoda oceny CAB – etap 1” określa minimalne czynności w zakresie przeglądu dokumentacji, gotowości i projektu, oczekiwane od CAB przed przystąpieniem do badania wdrożenia i skuteczności operacyjnej.
- 6 Kolumna „Metoda oceny CAB – etap 2” określa minimalne czynności w zakresie wdrożenia, skuteczności operacyjnej, doboru próby, badań, inspekcji lub weryfikacji dowodów, oczekiwane od CAB podczas oceny etapu 2 prowadzonej na miejscu lub w inny nadzorowany sposób.
- 7 CAB powinna stosować ogólne zasady, reguły dotyczące dowodów, podejście do doboru próby, zasady polegania na dowodach zewnętrznych, zasady raportowania oraz zasady zaliczenia/niezaliczenia określone w GP-03/Annex B do wszystkich wymagań wymienionych w tabeli.
- 8 Jeżeli w tabeli określono czynności oceny w sposób bardziej szczegółowy niż GP-03/Annex B, czynności te należy stosować jako właściwą dla danych kryteriów implementację GP-03/Annex B w odniesieniu do odpowiedniego wymagania. Jeżeli GP-03/Annex B zawiera dodatkowe wymagania ogólne niepowtórzone w tabeli, wymagania te mają w pełni zastosowanie.

- 9 Metody oceny określone w tabeli stanowią minimalny oczekiwany zakres prac audytowych dla każdego mającego zastosowanie wymagania. CAB może wykonać dodatkowe procedury, jeżeli jest to uzasadnione ryzykiem, złożonością, incydentami, zmianami, outsourcingiem, wcześniejszymi ustaleniami, niewystarczającymi dowodami lub potrzebą uzyskania wystarczających i odpowiednich dowodów obiektywnych.
- 10 Każde odstępstwo od metody oceny określonej w tabeli powinno zostać udokumentowane w zapisach z audytu i uzasadnione przez CAB. CAB powinna wykazać, że metoda alternatywna zapewnia co najmniej równoważne uzasadnienie zaufania dla odpowiedniego wymagania.
- 11 Dla każdego mającego zastosowanie wymagania CAB powinna udokumentować decyzję o możliwości zastosowania, przejrzone dowody, dobraną próbę, wykonane czynności audytowe, wynik oceny, ustalenia oraz wszelkie działania korygujące zgodnie z GP-03/Annex B.