

G-05

System Certyfikacji PL Portfela EUDI
Wymagania akredytacyjne dla jednostek
oceny zgodności (CAB)

WERSJA 1.01

2026.07.11

Oznaczenie dokumentu	G-05
Wersja	1.01
Status	Final
Data	11.07.2026
Rodzaj dokumentu	Dokument ramowy
Ramy nadrzędne	brak
Właściciel programu	Rzeczpospolita Polska / Minister Cyfryzacji
Przedmiot certyfikacji	Rozwiązanie Portfela EUDI
Odbiorcy pierwotni	Właściciel systemu/programu, jednostki CAB, NAB
Odbiorcy wtórni	Interesariusze ekosystemu Portfela EUDI
Poziom uzasadnienia zaufania <potwierdzenie tożsamości, CIR 2015/1502> lub <ocena, rozporządzenie (UE) 2019/881>	Nie dotyczy
Dokumenty podrzędne	GP-01, GP-02, GP-03

Historia zmian

Lp.	Zmiana	Wersja	Data
1.	Wersja oficjalna	1.0	2026-06-11
2.	Zmiany redakcyjne; część sekcji 7.9 (dotyczącej działań związanych z nadzorem dla certyfikatu najwyższego poziomu) przeniesiono do GP-03	1.01	2026-07-11

Spis treści

WPROWADZENIE	6
1 ZAKRES	7
2 ODNIESIENIA	8
2.1 Podstawa prawna	8
2.2 Odniesienia normatywne	8
2.3 Dokumenty równorzędne	9
2.4 Dokumenty podrzędne	9
3 TERMINY I DEFINICJE	10
3.1 Terminy	10
3.2 Skróty	11
4 WYMAGANIA OGÓLNE	12
4.1 Zagadnienia prawne i umowne	12
4.1.1 Odpowiedzialność prawna	12
4.1.2 Umowa dotycząca certyfikacji	12
4.1.3 Wykorzystywanie licencji, certyfikatów i znaków zgodności	12
4.2 Zarządzanie bezstronnością	12
4.3 Odpowiedzialność i finansowanie	13
4.4 Warunki niedyskryminujące	13
4.5 Poufność	13
4.6 Informacje dostępne publicznie	13
5 WYMAGANIA DOTYCZĄCE STRUKTURY	14
5.1 Struktura organizacyjna i najwyższe kierownictwo	14
5.2 Mechanizm zabezpieczania bezstronności	14
6 WYMAGANIA DOTYCZĄCE ZASOBÓW	15
6.1 Personel jednostki oceniającej zgodność	15
6.1.1 Postanowienia ogólne	15
6.1.2 Zarządzanie kompetencjami personelu zaangażowanego w proces certyfikacji	15
6.1.3 Umowa z personelem	16
6.2 Zasoby do oceny	16
6.2.1 Zasoby wewnętrzne	16
6.2.2 Zasoby zewnętrzne	17
7 WYMAGANIA DOTYCZĄCE PROCESU	18
7.1 Wymagania ogólne	18
7.1.1 Przedmiot certyfikacji	18
7.1.2 Ramy systemu certyfikacji	18
7.1.3 Hierarchia certyfikacji	19
7.1.4 Program certyfikacji	21

7.2	Wniosek.....	21
7.3	Przegląd wniosku	21
7.4	Ocena	22
7.5	Przegląd	22
7.6	Decyzja w sprawie certyfikacji.....	22
7.7	Dokumentacja certyfikacyjna.....	22
7.8	Katalog certyfikowanych wyrobów	23
7.9	Nadzór.....	23
7.10	Zmiany wpływające na certyfikację.....	24
7.11	Zakończenie, ograniczenie, zawieszenie lub cofnięcie certyfikacji.....	26
7.12	Zapisy.....	27
7.13	Skargi i odwołania.....	27
8	WYMAGANIA DOTYCZĄCE SYSTEMU ZARZĄDZANIA.....	28
8.1	Opcje	28
8.2	Ogólna dokumentacja systemu zarządzania	28
8.3	Nadzór nad dokumentami	28
8.4	Nadzór nad zapisami.....	28
8.5	Przegląd zarządzania.....	28
8.6	Audyty wewnętrzne.....	28
8.7	Działania korygujące	28
8.8	Działania zapobiegawcze.....	28
9	DODATKOWE POSTANOWIENIA DOTYCZĄCE WYMAGAŃ AKREDYTACYJNYCH DLA CAB-ITSEF	29
10	OKRES PRZEJŚCIOWY.....	29
	ZAŁĄCZNIK A. WYMAGANIA KOMPETENCYJNE DLA ROZWIĄZANIA PORTFELA EUDI.....	31

Wprowadzenie

- 1 Celem dokumentu jest spełnienie ogólnych wymagań społeczności międzynarodowej dotyczących zapewnienia zaufania i pewności w odniesieniu do rozwiązań europejskiego portfela tożsamości cyfrowej, w tym m.in. mających zastosowanie wymagań rozporządzenia (UE) 910/2014.
- 2 Dokument ma na celu wsparcie krajowych jednostek akredytujących określonych w rozporządzeniu (UE) 765/2008 w stosowaniu PN-EN ISO/IEC 17065 wraz z rozszerzeniami na potrzeby akredytacji jednostek oceniających zgodność (CAB) uczestniczących w systemie certyfikacji PL portfela EUDI.
- 3 Dokument nie powtarza wymagań PN-EN ISO/IEC 17065, lecz podąża za strukturą tego dokumentu.
- 4 Dodatkowo dokument uwzględnia wymagania dotyczące audytu systemów zarządzania, zdefiniowane w PN-EN ISO/IEC 17021-1 i PN-EN ISO/IEC 27006-1. Wymagania te są włączone pośrednio poprzez odniesienia do ETSI EN 319 403-1 i mają zastosowanie do GP-03.

1 Zakres

- 5 Niniejszy dokument zawiera wymagania dotyczące kompetencji, spójnego działania i bezstronności jednostek oceniających zgodność wykonujących ocenę i certyfikację rozwiązania europejskiego portfela tożsamości cyfrowej na mocy rozporządzenia (UE) 2024/2981, w uzupełnieniu wymagań zawartych w PN-EN ISO/IEC 17065 oraz — w stosownych przypadkach — PN-EN ISO/IEC 17025.
- 6 CAB-CB musi być akredytowana zgodnie z PN-EN ISO/IEC 17065 w zakresie właściwych krajowych programów certyfikacji. Dodatkowo w określonych programach CAB-ITSEF musi być akredytowana zgodnie z PN-EN ISO/IEC 17025. Oba rodzaje CAB muszą być akredytowane przez krajową jednostkę akredytującą wyznaczoną na podstawie rozporządzenia (UE) nr 765/2008.
- 7 Rozszerzenia PN-EN ISO/IEC 17065 określone w niniejszym dokumencie mają zastosowanie do wszystkich programów certyfikacji, tj. GP-01, GP-02 i GP-03.
- 8 17065-01 GP-02: Rozszerzenia PN-EN ISO/IEC 17065 właściwe dla programu certyfikacji EUCC mają zastosowanie z ograniczeniem do obszaru kompetencji „oprogramowanie ogólne i urządzenia sieciowe”.
- 9 Rozszerzenia PN-EN ISO/IEC 17065 odnoszące się do ETSI EN 319 403-1 mają zastosowanie wyłącznie do GP-03.
- 10 Dodatkowo w rozdziale 9 określono rozszerzenia PN-EN ISO/IEC 17025 właściwe dla CAB-ITSEF, mające zastosowanie do dwóch programów certyfikacji, tj. GP-01 i GP-02.

2 Odniesienia

2.1 Podstawa prawna

- 11 System certyfikacji PL Portfela EUDI został wprowadzony przez właściwy polski akt prawny.

2.2 Odniesienia normatywne

- 12 Poniższe dokumenty powołane są niezbędne do stosowania niniejszego dokumentu. W przypadku powołań datowanych zastosowanie ma wyłącznie wydanie cytowane; w przypadku powołań niedatowanych zastosowanie ma najnowsze wydanie dokumentu powołanego (łącznie ze zmianami).
- 13 PN-EN ISO/IEC 17000, Ocena zgodności — Terminologia i zasady ogólne
- 14 PN-EN ISO/IEC 17021-1, Ocena zgodności — Wymagania dla jednostek prowadzących audit i certyfikację systemów zarządzania, Część 1: Wymagania
- 15 PN-EN ISO/IEC 17025, Ocena zgodności — Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących
- 16 PN-EN ISO/IEC 17065, Ocena zgodności — Wymagania dla jednostek certyfikujących wyroby, procesy i usługi
- 17 PN-EN ISO/IEC 17067, Ocena zgodności — Podstawy certyfikacji wyrobów oraz wytyczne dotyczące programów certyfikacji wyrobów
- 18 PN-EN ISO/IEC 19896-1, Wymagania dotyczące kompetencji personelu jednostek oceniających zgodność w zakresie bezpieczeństwa IT, Część 1: Przegląd i pojęcia
- 19 PN-EN ISO/IEC 19896-3, Wymagania dotyczące kompetencji personelu jednostek oceniających zgodność w zakresie bezpieczeństwa IT, Część 3: Wymagania dotyczące wiedzy i umiejętności oceniających i przeglądających według serii PN-EN ISO/IEC 15408 oraz PN-EN ISO/IEC 18045
- 20 PN-EN ISO/IEC 27006-1, Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności — Wymagania dla jednostek prowadzących audit i certyfikację systemów zarządzania bezpieczeństwem informacji, Część 1: Postanowienia ogólne

21 ETSI EN 319 403-1, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers (Ocena zgodności dostawców usług zaufania — Część 1: Wymagania dla jednostek oceniających zgodność oceniających dostawców usług zaufania)

22 PN-EN 17640:2022 + A1:2026, Ograniczona w czasie metodyka oceny cyberbezpieczeństwa produktów teleinformatycznych (FITCEM)

2.3 Dokumenty równorzędne

23 G-01. System certyfikacji PL Portfela EUDI

24 G-02. Słownik

25 G-03. Organizacja i wsparcie właściciela krajowych programów certyfikacji EUDI

26 G-04. Opracowanie i utrzymanie rejestru ryzyka dla wdrożenia i certyfikacji Portfela EUDI

2.4 Dokumenty podrzędne

27 GP-01. Program certyfikacji funkcjonalnej Portfela EUDI

28 GP-02. Program certyfikacji cyberbezpieczeństwa

29 GP-03. Program certyfikacji eID

3 Terminy i definicje

3.1 Terminy

30 Na potrzeby niniejszego dokumentu wszystkie terminy i definicje podano w G-02 Słownik.

31 Ponadto zastosowanie mają terminy i definicje z:

- o PN-EN ISO/IEC 17000
- o ETSI EN 319 403-1

32 oraz następujące.

33 **kompetencje** — zdolność stosowania wiedzy, umiejętności i doświadczenia określonych w programie certyfikacji w celu osiągnięcia zamierzonego wyniku

34 [ŹRÓDŁO: PN-EN ISO/IEC 24765:2017, 3.676, zmodyfikowane — sformułowanie „oraz odpowiednich cech osobistych” zastąpiono „doświadczenia”; dodano sformułowanie „w celu osiągnięcia zamierzonego wyniku”]

35 **ciągłość uzasadnienia zaufania (assurance continuity)** — podejście wdrożone w systemie certyfikacji w celu utrzymania poziomu bazowego uzasadnienia zaufania w certyfikowanym obiekcie.

36 [ŹRÓDŁO: przyjęte z rozporządzenia wykonawczego Komisji nr 2024/482, załącznik IV]

37 **poziom bazowy uzasadnienia zaufania (assurance baseline)** — zwięzienie działań wykonanych zarówno przez oceniającego, jak i dewelopera, skutkujących certyfikowanym obiektem, zarejestrowanych lub przedłożonych jako dowody i mierzalnych poprzez zmiany tych dowodów

38 ¹ [ŹRÓDŁO: Assurance continuity: CCRA requirements, 2.2 i), zmodyfikowane — „TOE” zastąpiono „obiektem”]

39 **zmiana duża (major change)** — zmiana, która wpływa na poziom bazowy uzasadnienia zaufania rozwiązywania Portfela EUDI

¹ <https://www.commoncriteriaportal.org/files/operatingprocedures/CCDB-014-v3.1-2024-February-29-Final-Assurance-Continuity.pdf> (dostęp 27.04.2026)

40 UWAGA 1 do hasła: Niezgodności mogą skutkować zmianami (dużymi lub
małymi).

41 UWAGA 2 do hasła: Zmiany mogą wynikać z incydentów, podatności lub
nowych opracowań.

42 [ŹRÓDŁO: adaptacja na podstawie Assurance continuity: CCRA
requirements, rozdział 3]

43 **zmiana mała (minor change)** — zmiana, która nie wpływa na poziom
bazowy uzasadnienia zaufania rozwiązania Portfela EUDI

44 PRZYKŁAD:

- o zmiany środowiska ICT, które nie zmieniają certyfikowanego obiektu,
- o zmiany certyfikowanego obiektu, które nie wpływają na dowody uzasadnienia zaufania,
- o zmiany środowiska deweloperskiego.

UWAGA 1 do hasła: Zbiór zmian małych łącznie może mieć duży wpływ na funkcjonalność lub bezpieczeństwo, a tym samym skutkować zmianą dużą.

45 [ŹRÓDŁO: adaptacja na podstawie Assurance continuity: CCRA
requirements, rozdział 3]

3.2 Skróty

46 Na potrzeby dokumentu zastosowanie mają następujące skróty:

47 CAB-CB jednostka oceniająca zgodność — jednostka certyfikująca
(Conformity Assessment Body – Certification Body)

48 CAB-ITSEF jednostka oceniająca zgodność — laboratorium badawcze
(Conformity Assessment Body – IT Security Evaluation Facility)

49 EC Komisja Europejska (European Commission)

50 EU Unia Europejska (European Union)

51 EUDI europejska tożsamość cyfrowa (European Digital
Identification)

52 ICT technologie informacyjno-komunikacyjne (Information and
Communications Technology)

53	IT	teleinformatyka (Information Technology)
54	PID	dane identyfikujące osobę (Personal Identification Data)
55	TSP	dostawca usług zaufania (Trusted Service Provider)

4 Wymagania ogólne

4.1 Zagadnienia prawne i umowne

4.1.1 Odpowiedzialność prawna

56 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 4.1.1.

4.1.2 Umowa dotycząca certyfikacji

57 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 4.1.2. Ponadto zastosowanie mają następujące wymagania.

58 4.1.2.1 Wnioskodawca/posiadacz certyfikatu musi na żądanie udostępnić CAB-CB lub Właścicielowi systemu wszystkie informacje oraz wszelką dokumentację potwierdzającą ciągłą zgodność z mającymi zastosowanie wymaganiami certyfikacyjnymi. Informacje muszą być przekazywane bez zwłoki.

4.1.3 Wykorzystywanie licencji, certyfikatów i znaków zgodności

59 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 4.1.3. Ponadto zastosowanie mają następujące wymagania.

60 4.1.3.1 Zastosowanie ma wyłącznie znak zgodności zdefiniowany w G-03. W ramach programów certyfikacji GP-01, GP-02 i GP-03 (z wyjątkiem certyfikatu najwyższego poziomu) nie mogą być stosowane żadne dodatkowe znaki zgodności.

61 4.1.3.2 CAB-CB musi przyjąć odpowiedzialność za przyznawanie, zawieszanie i cofanie prawa do używania znaku zgodności zgodnie z decyzją certyfikacyjną.

4.2 Zarządzanie bezstronnością

62 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 4.2.

63 Dodatkowo wymagania specyficzne dla przedmiotu certyfikacji w poszczególnych programach certyfikacji, tj. GP-01, GP-02 i GP-03, są zawarte w tych dokumentach.

4.3 Odpowiedzialność i finansowanie

64 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 4.3.

4.4 Warunki niedyskryminujące

65 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 4.4.

4.5 Poufność

66 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 4.5. Ponadto zastosowanie mają następujące wymagania.

67 4.5.1 CAB-CB musi przekazać raport z certyfikacji Właścicielowi programu.

68 4.5.2 CAB-CB musi wdrożyć niezbędne i odpowiednie środki techniczne i organizacyjne w celu zapewnienia poufności wszystkich informacji uzyskanych lub wytworzonych w trakcie wykonywania działań certyfikacyjnych, w tym informacji dotyczących praw własności intelektualnej. Środki te muszą mieć zastosowanie do całego personelu oraz innych osób, którym przyznano dostęp do takich informacji.

4.6 Informacje dostępne publicznie

69 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 4.6.

5 Wymagania dotyczące struktury

5.1 Struktura organizacyjna i najwyższe kierownictwo

70 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 5.1.

5.2 Mechanizm zabezpieczania bezstronności

71 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 5.2.

6 Wymagania dotyczące zasobów

6.1 Personel jednostki oceniającej zgodność

6.1.1 Postanowienia ogólne

72 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 6.1.1.

6.1.2 Zarządzanie kompetencjami personelu zaangażowanego w proces certyfikacji

73 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 6.1.2. Ponadto zastosowanie mają następujące wymagania i wytyczne.

74 6.1.2.1 CAB-CB musi zapewnić i zweryfikować, że posiada wiedzę w zakresie:

75 a) szczegółowej i technicznej wiedzy o właściwych architekturach rozwiązania portfela oraz systemu identyfikacji elektronicznej;

76 b) stosowania konkretnych norm związanych z programem certyfikacji zgodnie z 7.1.2;

77 c) zagrożeń i ryzyk właściwych dla tych architektur;

78 d) dostępnych rozwiązań bezpieczeństwa i ich właściwości zgodnie z załącznikiem do rozporządzenia wykonawczego (UE) 2015/1502;

79 e) działań związanych z certyfikacją funkcjonalną i certyfikacją cyberbezpieczeństwa komponentów rozwiązania portfela oraz powiązanego systemu identyfikacji elektronicznej;

80 f) mających zastosowanie krajowych programów certyfikacji.

81 Szczegółowe wymagania dotyczące kompetencji personelu zawarto w załączniku A (normatywnym).

82 6.1.2.2 CAB-CB musi ustanowić, wdrożyć i stosować system zarządzania kompetencjami dla właściwego personelu. Elementy kompetencji, poziomy kompetencji, wiedza, umiejętności i doświadczenie muszą być zgodne ze szczegółowymi wymaganiami zawartymi w PN-EN ISO/IEC 18896-1.

83 6.1.2.3 GP-02: Rozszerzenia PN-EN ISO/IEC 17065 właściwe dla programu certyfikacji EUCC mają zastosowanie do CAB-CB z ograniczeniem do obszaru kompetencji „oprogramowanie ogólne i urządzenia sieciowe”.

84 6.1.2.4 GP-03: Zastosowanie mają dodatkowe wymagania ETSI EN 319 403-1, 6.1.2 dotyczące procesu audytu i związanych z nim kompetencji.

6.1.3 Umowa z personelem

85 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 6.1.3.

6.2 Zasoby do oceny

6.2.1 Zasoby wewnętrzne

86 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 6.2.1. Ponadto zastosowanie mają następujące wymagania.

87 6.2.1.1 Wymagania zawarte w ETSI EN 319 403-1, pkt 6.2.1.1 muszą być przyjęte w następujący sposób:

- o „TSP” zastępuje się „w obszarze usług związanych z rozwiązaniem Portfela EUDI”

88 6.2.1.2 Wymagania zawarte w ETSI EN 319 403-1, pkt 6.2.1.2 muszą być dostosowane w następujący sposób:

- o „TSP” i „usługi zaufania” zastępuje się „usługami związanymi z rozwiązaniem Portfela EUDI”

89 6.2.1.3 Wymagania zawarte w ETSI EN 319 403-1, pkt 6.2.1.3 muszą być dostosowane w następujący sposób:

- o „TSP” zastępuje się — odpowiednio — „dostawcą portfela EUDI” lub „dostawcą PID”,

90 6.2.1.4 Wymagania zawarte w ETSI EN 319 403-1, pkt 6.2.1.4 muszą być dostosowane w następujący sposób:

- o „audyty TSP” zastępuje się „audytami usług związanych z rozwiązaniem Portfela EUDI”,
- o „usługi zaufania” zastępuje się „usługami związanymi z rozwiązaniem Portfela EUDI, w tym zarządzaniem tożsamością”,
- o „TSP” zastępuje się — odpowiednio — „dostawcą portfela EUDI” lub „dostawcą PID”.

91 6.2.1.5 Wymagania zawarte w ETSI EN 319 403-1, pkt 6.2.1.5 muszą być dostosowane w następujący sposób:

o „oceny TSP” zastępuje się „ocenami SZBI (ISMS)”.

92 6.2.1.6 Zastosowanie mają wymagania zawarte w ETSI EN 319 403-1, pkt 6.2.1.6.

93 6.2.1.7 Wymagania zawarte w ETSI EN 319 403-1, pkt 6.2.1.7 i 6.1.8 muszą być dostosowane w następujący sposób:

o „TSP” i „usługa zaufania TSP” zastępuje się „usługami związanymi z rozwiązaniem Portfela EUDI”

94 6.2.1.9 Wymagania zawarte w ETSI EN 319 403-1, pkt 6.2.1.9 muszą być dostosowane w następujący sposób:

o „audyty TSP” zastępuje się „audytami SZBI (ISMS)”

6.2.2 Zasoby zewnętrzne

95 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 6.2.2. Ponadto zastosowanie mają następujące wymagania.

96 6.2.2.1 CAB-CB może zlecać działania oceniające jednostce trzeciej na następujących warunkach:

97 a) wszyscy podwykonawcy wykonujący działania oceniające muszą — w stosownych przypadkach i odpowiednio do wykonywanych zadań — spełniać właściwe normy zharmonizowane:

o PN-EN ISO/IEC 17025 dla badań zgodności i ewaluacji ocen bezpieczeństwa IT

o PN-EN ISO/IEC 17021-1 dla audytowania

98 b) musi zostać zachowana pełna odpowiedzialność za wszystkie działania związane z oceną, zlecone innym jednostkom.

99 c) muszą istnieć odpowiednie środki w ramach akredytacji CAB-CB, w tym poleganie na akredytacji CAB-ITSEF w GP-01 i GP-02.

100 d) należy ustanowić procedury dotyczące terminu i sposobu informowania właścicieli programów o wszelkich zleconych na zewnątrz działaniach związanych z oceną.

101 W GP-01 i GP-02 wymagane są CAB-ITSEF akredytowane zgodnie z PN-EN ISO/IEC 17025.

7 Wymagania dotyczące procesu

7.1 Wymagania ogólne

102 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.1.

103 Ponadto wymagania ETSI EN 319 403-1, 7.1 dostosowuje się w następujący sposób:

- o „TSP i usługa(-i) zaufania” zastępuje się — odpowiednio — „dostawcą portfela EUDI i usługami związanymi z rozwiązaniem Portfela EUDI” lub „dostawcą PID i usługami związanymi z rozwiązaniem Portfela EUDI”.

7.1.1 Przedmiot certyfikacji

104 Zgodnie z art. 3 ust. 3 CIR (UE) 2024/2981 przedmiot certyfikacji obejmuje następujące elementy:

105 a) komponenty programowe, w tym ustawienia i konfiguracje rozwiązań portfela oraz systemu identyfikacji elektronicznej, w ramach którego rozwiązania portfela są dostarczane;

106 b) komponenty sprzętowe i platformy, na których działają lub na których opierają się w zakresie operacji krytycznych komponenty programowe, o których mowa w lit. a), w przypadkach gdy są one dostarczane bezpośrednio lub pośrednio przez rozwiązanie portfela i system identyfikacji elektronicznej, w ramach którego są dostarczane, oraz gdy są wymagane do osiągnięcia pożądanego poziomu uzasadnienia zaufania dla tych komponentów programowych;

107 c) procesy wspierające dostarczanie i działanie rozwiązania portfela, w tym proces onboarding użytkownika, o którym mowa w art. 5a rozporządzenia (UE) nr 910/2014, obejmujący co najmniej rejestrację, zarządzanie środkami elektronicznymi i organizację zgodnie z pkt 2.1, 2.2 i 2.4 załącznika I do rozporządzenia wykonawczego (UE) 2015/1502.

7.1.2 Ramy systemu certyfikacji

108 System certyfikacji składa się z wielu programów certyfikacji, z których każdy obejmuje określone aspekty ogólnych ram. Dla każdego przedmiotu certyfikacji ustanawia się konkretny program certyfikacji, obejmujący mające zastosowanie wymagania dotyczące wyrobu lub usługi. Wszystkie programy oparte są na PN-EN ISO/IEC 17065 jako normie oceny zgodności. Programy wymieniono w Tabeli 1.

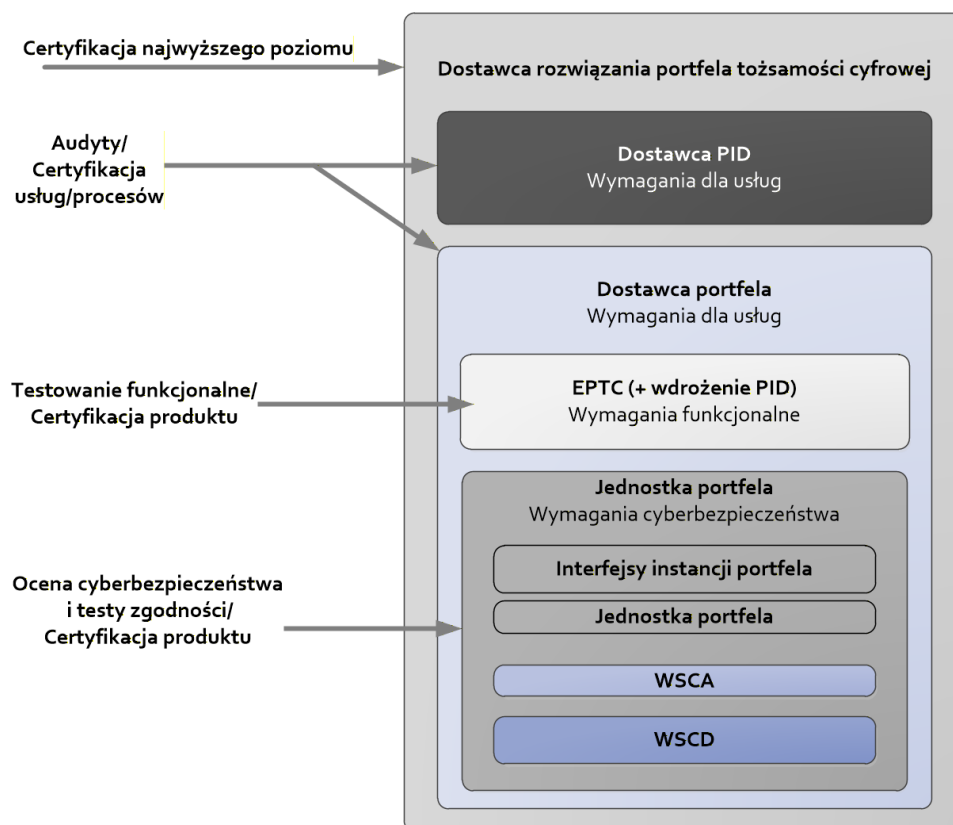
Tabela 1 Ramy systemu certyfikacji

Przedmiot certyfikacji	Program certyfikacji	Metoda oceny	Wymagania dotyczące wyrobu lub usługi	Wnioskodawca
Dostarczanie rozwiązania Portfela EUDI (usługa)	GP-03	Audyt	WZ-03-01 WZ-03-03 WP-03-01 WP-03-03	Dostawca Portfela EUDI
Dostarczanie portfeli EUDI użytkownikom końcowym (usługa)	GP-03	Audyt	WZ-03-01 WP-03-01 WP-03-02	Dostawca Portfela EUDI
Wydawanie PID użytkownikom końcowym portfela (usługa)	GP-03	Audyt	WZ-03-01 WZ-03-02 WP-03-01	Dostawca PID
Cyberbezpieczeństwo rozwiązania portfela (wyrób)	GP-02	Ocena bezpieczeństwa IT	WP-02-01 WP-02-02 WP-02-03	Dostawca Portfela EUDI
Funkcjonalność rozwiązania portfela (wyrób)	GP-01	Badania	WP-01-01	Dostawca Portfela EUDI

7.1.3 Hierarchia certyfikacji

109

Certyfikacja rozwiązania Portfela EUDI musi przebiegać zgodnie z hierarchią certyfikacji składającą się z certyfikacji najwyższego poziomu wspieranej przez podrzędne certyfikacje na poziomie programów, przyznawane odpowiednim dostawcom. Hierarchię zilustrowano na Rysunek 1.



110

Rysunek 1 Relacje między poszczególnymi obiektami w systemie certyfikacji

111 Dostawca krajowego rozwiązania Portfela EUDI musi posiadać ważny certyfikat najwyższego poziomu, a Właściciel systemu musi zapewnić jego notyfikację Komisji Europejskiej zgodnie z art. 5d rozporządzenia (UE) nr 910/2014. Certyfikacja ta musi obejmować system identyfikacji elektronicznej w całości, w tym rozwiązanie portfela, rozwiązania w zakresie ładu organizacyjnego, ramy zaufania oraz zgodność wszystkich dostawców działających w ramach systemu. Certyfikacja najwyższego poziomu musi być oceniana względem wymagań określonych w GP-03 i musi opierać się na ważnych certyfikacjach na poziomie programów, które zostały przyznane dostawcom.

112 Każdy dostawca usług w ramach właściwego programu musi posiadać ważną certyfikację obejmującą wymagania mające zastosowanie do jego wyznaczonej roli. Przypisanie wymagań do ról jest określone w mających zastosowanie dokumentach programów certyfikacji (serie GP-01, GP-02 i GP-03). Jeżeli podmiot pełni wiele ról, musi posiadać certyfikację dla każdego wyrobu lub usługi.

113 Wykonując działania oceniające na potrzeby certyfikacji najwyższego poziomu, CAB-CB może polegać na certyfikacjach na poziomie programów jako informacjach o uzasadnieniu zaufania, zgodnie z G-01. W przypadku

polegania na takich certyfikacjach CAB-CB musi zweryfikować ich ważność i zakres oraz nie może ponownie oceniać wymagań już objętych tymi certyfikacjami.

114 Właściciel systemu musi zapewnić, aby dostawca Portfela EUDI lub dostawca PID w ramach systemu mieli możliwość otrzymania certyfikatów oraz aby programy pozostawały zgodne z wymaganiami. Jeżeli dostawca przestaje dysponować ważnym certyfikatem, certyfikacja najwyższego poziomu musi zostać zaktualizowana, aby odzwierciedlić tę zmianę. Certyfikacja najwyższego poziomu nie może być wydana ani utrzymywana, jeżeli brakuje ważnej certyfikacji dla któregośkolwiek z komponentów wchodzących w skład rozwiązania Portfela EUDI (wyrobu lub usługi).

115 Certyfikat najwyższego poziomu nie może być wydany ani utrzymywany, o ile wszystkie elementy przedmiotu certyfikacji określone w pkt 7.1.1 nie są objęte ważnymi certyfikatami przyznanymi dostawcom.

7.1.4 Program certyfikacji

116 Dla każdego elementu przedmiotu certyfikacji CAB-CB musi prowadzić program certyfikacji zgodny z programem certyfikacji wyrobów typu 5 oraz certyfikacją usług typu 6 zgodnie z definicjami PN-EN ISO/IEC 17067. Proces certyfikacji musi obejmować:

117 II. określenie właściwości poprzez badania i audyt (zob. 7.4);

118 III. przegląd informacji i wyników oceny (zob. 7.5);

119 IV. decyzje w sprawie certyfikacji: przyznanie, utrzymywanie, rozszerzanie, ograniczanie, zawieszanie i cofanie certyfikacji (zob. 7.6);

120 V. atestację, licencjonowanie, wydanie certyfikatu oraz przyznanie prawa do używania certyfikatów i znaków (zob. 7.7);

121 VI. nadzór, ocenę działania procesu oraz audyt systemu zarządzania (zob. 7.9).

7.2 Wniosek

122 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.2.

7.3 Przegląd wniosku

123 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.3.

124 Ponadto zastosowanie mają następujące wymagania.

125 7.3.1 Jeżeli mający zastosowanie program certyfikacji wymaga, aby
wnioskodawca posiadał ważne certyfikaty w ramach innych programów
certyfikacji, CAB-CB musi — w ramach przeglądu wniosku —
zweryfikować istnienie, ważność i zakres tych certyfikatów. W przypadku
gdy procesy oceny i certyfikacji w ramach GP-01 lub GP-02 są w toku, CAB-
CB musi — na podstawie deklaracji wnioskodawcy — ustalić, czy ich status
nie ogranicza rozpoczęcia procesu w ramach programu certyfikacji GP-03.
CAB-CB musi zarejestrować podstawę swojego ustalenia.

7.4 Ocena

126 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.4.

127 Ponadto zastosowanie mają następujące wymagania.

128 7.4.1 Wymagania zawarte w ETSI EN 319 403-1, pkt 7.4.1, 7.4.2, 7.4.3, 7.4.4,
7.4.5, muszą być dostosowane w następujący sposób:

- o „TSP” zastępuje się — odpowiednio — „dostawcą portfela EUDI” lub
„dostawcą PID” oraz świadczeniem ich usług,
- o „usługi zaufania” zastępuje się „usługami związanymi z
rozwiązaniem Portfela EUDI”

7.5 Przegląd

129 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.5.

130 7.5.1 Zastosowanie mają wymagania ETSI EN 319 403-1, 7.5.

7.6 Decyzja w sprawie certyfikacji

131 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.6.

7.7 Dokumentacja certyfikacyjna

132 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.7.

133 Ponadto zastosowanie mają następujące wymagania.

134 7.7.1 Dokumentacja certyfikacyjna musi zawierać:

- 135 a) unikalny kod identyfikacyjny;
- 136 b) nazwę i wersję przedmiotu certyfikacji;

- 137 c) nazwę systemu identyfikacji elektronicznej oraz państwo członkowskie,
w stosownych przypadkach;
- 138 d) nazwę, adres i dane kontaktowe wnioskodawcy;
- 139 e) łącze do strony internetowej wnioskodawcy zawierającej informacje,
które muszą być publicznie dostępne zgodnie z 4.6;
- 140 f) nazwę, adres i dane kontaktowe CAB-CB;
- 141 h) nazwę Właściciela programu;
- 142 i) odniesienia do rozporządzenia (UE) 910/2014 oraz do rozporządzenia
(UE) 2024/2981;
- 143 j) odniesienie do publicznego raportu z certyfikacji;
- 144 k) odniesienie do norm użytych do oceny, wraz z ich wersjami; tj. mającą
zastosowanie wersję każdego dokumentu serii GP, względem którego
przeprowadzono ocenę;
- 145 m) zakres certyfikacji, w tym wszelkie ograniczenia;
- 146 n) nazwę dostawcy portfela EUDI lub dostawcy PID;
- 147 o) poziom uzasadnienia zaufania.

148 7.7.2 CAB-CB musi wydać nową dokumentację certyfikacyjną, jeżeli ocena
— w tym nadzór lub ponowne oceny — zidentyfikuje zmiany przedmiotu
certyfikacji. Nowa dokumentacja certyfikacyjna musi zachować datę
wygaśnięcia pierwotnej dokumentacji certyfikacyjnej.

7.8 Katalog certyfikowanych wyrobów

149 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.8.

150 Ponadto zastosowanie mają następujące wymagania.

151 7.8.1 CAB-CB musi powiadamiać Właściciela programu o wydaniu,
zakończeniu (na życzenie klienta), zawieszeniu i cofnięciu certyfikatu.

7.9 Nadzór

152 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.9.

153 7.9.1 Wymagania zawarte w ETSI EN 319 403-1, 7.9 muszą być
dostosowane w następujący sposób:

- o „TSP” zastępuje się — odpowiednio — „dostawcą portfela EUDI” lub „dostawcą PID” oraz „świadczeniem ich usługi”.

154 Ponadto zastosowanie mają następujące wymagania.

155 7.9.2 CAB-CB musi zapewnić, aby działania nadzorcze obejmowały weryfikację, że:

156 a) posiadacz certyfikatu przestrzega mającego zastosowanie programu certyfikacji określonego w 7.1.2 oraz krajowych programów certyfikacji;

157 b) certyfikowany przedmiot certyfikacji nadal spełnia wymagania określone w 7.1.2 oraz w krajowych programach certyfikacji.

158 7.9.3 CAB-CB musi także prowadzić działania nadzorcze na podstawie następujących informacji:

159 a) informacji od krajowych jednostek akredytujących oraz właściwych organów nadzoru rynku;

160 b) informacji wynikających z audytów i postępowań wyjaśniających prowadzonych przez jednostkę certyfikującą lub inne właściwe organy;

161 c) skarg i odwołań.

162 7.9.4 CAB-CB może przeprowadzać oceny specjalne. Ocena specjalna może zostać zainicjowana na wniosek posiadacza certyfikatu albo przez CAB-CB w odpowiedzi na konkretny problem, taki jak zgłoszenie podatności lub informacja otrzymana od organu nadzoru lub organu nadzoru rynku.

163 7.9.5 Zakres oceny specjalnej musi być jasno zdefiniowany i ograniczony do działań niezbędnych do rozwiązania konkretnego problemu, który ją wywołał.

164 **7.10 Zmiany wpływające na certyfikację**

164 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.10.

165 Ponadto zastosowanie mają następujące wymagania.

166 7.10.1 Wymagania zawarte w ETSI EN 319 403-1, pkt 7.4.0–7.4.7, muszą być dostosowane w następujący sposób:

- o „TSP” zastępuje się — odpowiednio — „dostawcą portfela EUDI” lub „dostawcą PID” oraz świadczeniem ich usługi.

- 167 7.10.2 CAB-CB musi wykonywać działania oceniające w następstwie zmian
programu certyfikacji, obejmujących:
- 168 a) rewizję programu certyfikacji;
- 169 b) publikację nowych specyfikacji lub norm; lub
- 170 c) publikację nowych wersji takich specyfikacji lub norm.
- 171 7.10.3 CAB-CB musi podejmować odpowiednie działania zgodnie z
informacjami przekazanymi przez Właściciela programu.
- 172 7.10.4 CAB-CB musi wykonywać działania oceniające w następstwie
innych zmian wpływających na certyfikację, obejmujących:
- 173 a) dodanie nowego dostawcy portfela lub dostawcy PID do systemu albo
usunięcie istniejącego dostawcy portfela lub dostawcy PID z systemu, w
stosownych przypadkach;
- 174 b) zmianę tożsamości lub statusu prawnego istniejącego dostawcy portfela
lub dostawcy PID w ramach systemu, w stosownych przypadkach;
- 175 c) istotne zmiany architektury lub projektu rozwiązania portfela;
- 176 d) istotne zmiany procesów rejestracji lub potwierdzania tożsamości;
- 177 e) poważny incydent bezpieczeństwa;
- 178 f) zawieszenie lub cofnięcie certyfikacji powiązanych komponentów
certyfikowanych przez tę samą lub inne akredytowane jednostki
certyfikujące (zob. 7.4.2)
- 179 g) istotne zmiany rejestru ryzyka programu.
- 180 7.10.5 CAB-CB musi ustanowić, wdrożyć i utrzymywać proces zarządzania
zmianami przedmiotu certyfikacji oraz warunków, na jakich przyznano
certyfikację.
- 181 7.10.6 CAB-CB musi ustalić, czy zmiany przedmiotu certyfikacji lub
środowiska zagrożeń wymagają dodatkowych działań oceniających. Ocena
specjalna może również zostać zainicjowana na wniosek posiadacza
certyfikatu.
- 182 7.10.7 CAB-CB musi określić i wdrożyć odpowiednie działania w
odpowiedzi na takie zmiany. Działania te muszą obejmować, w stosownych
przypadkach:

- 183 a) dodatkowe działania oceniające;
- 184 b) przegląd wyników oceny;
- 185 c) wydanie zaktualizowanej dokumentacji certyfikacyjnej;
- 186 d) zmiany działań nadzorczych.
- 187 7.10.8 CAB-CB musi zarejestrować uzasadnienie wyłączenia
któregokolwiek z tych działań.

7.11 Zakończenie, ograniczenie, zawieszenie lub cofnięcie certyfikacji

- 188 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.11.
- 189 Ponadto zastosowanie mają następujące wymagania.
- 190 7.11.1 Jeżeli wymagania certyfikacyjne nie są spełnione, CAB-CB musi:
- 191 a) poinformować posiadacza certyfikatu o każdej niezgodności i zażądać
podjęcia odpowiednich działań naprawczych;
- 192 b) powiadomić właściwe organy nadzoru rynku, gdy niezgodność dotyczy
mającego zastosowanie prawodawstwa unijnego;
- 193 c) zapewnić, aby posiadacz certyfikatu został poinformowany o
warunkach:
- o przeprowadzenia działań naprawczych,
 - o zawieszenia certyfikacji oraz przywrócenia certyfikacji po usunięciu
niezgodności,
 - o cofnięcia certyfikacji.
- 194 7.11.2 CAB-CB musi bez zbędnej zwłoki zawiesić certyfikację po
potwierdzeniu, że zgłoszone naruszenie bezpieczeństwa lub
kompromitacja wpływa na zgodność z mającym zastosowanie krajowym
programem certyfikacji.
- 195 7.11.3 CAB-CB musi cofnąć zawieszoną certyfikację, jeżeli niezbędne
działania korygujące nie zostały zakończone w odpowiednim terminie.

196 7.11.4 CAB-CB musi cofnąć certyfikację, jeżeli zidentyfikowana podatność
nie została usunięta w odpowiednim czasie, z uwzględnieniem jej wagi i
potencjalnego wpływu.

197 7.11.5 Ponadto podstawą zawieszenia lub cofnięcia muszą być następujące
warunki:

198 a) certyfikacja w ramach programu certyfikacji GP-01, GP-02 lub GP-03
została zawieszona lub cofnięta, a w ramach systemu nie jest dostępne
żadne alternatywne certyfikowane rozwiązanie portfela;

199 b) Właściciel programu nie jest w stanie wykazać ciągłej zgodności z
wymaganiami ładu organizacyjnego określonymi w G-01.

7.12 Zapisy

200 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.12. Ponadto
zastosowanie mają następujące wymagania.

201 7.12.1 Zapisy muszą być przechowywane zgodnie z G-01, pkt 5.10.

7.13 Skargi i odwołania

202 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 7.13. Ponadto
zastosowanie mają następujące wymagania.

203 7.13.1 CAB-CB musi przekazywać Właścicielowi programu wszelkie skargi
lub odwołania, których nie można rozstrzygnąć, do dalszej oceny i
rozstrzygnięcia.

8 Wymagania dotyczące systemu zarządzania

8.1 Opcje

204 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 8.1.

8.2 Ogólna dokumentacja systemu zarządzania

205 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 8.2.

8.3 Nadzór nad dokumentami

206 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 8.3.

8.4 Nadzór nad zapisami

207 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 8.4.

8.5 Przegląd zarządzania

208 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 8.5.

8.6 Audyty wewnętrzne

209 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 8.6.

8.7 Działania korygujące

210 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 8.7.

8.8 Działania zapobiegawcze

211 Zastosowanie mają wymagania PN-EN ISO/IEC 17065, 8.8.

9 Dodatkowe postanowienia dotyczące wymagań akredytacyjnych dla CAB-ITSEF

212 Dla GP-01 i GP-02 CAB-ITSEF musi być akredytowana zgodnie z PN-EN ISO/IEC 17025 w zakresie wynikającym z charakterystyki obiektu certyfikacji.

213 Ponadto zastosowanie mają następujące wymagania.

214 CAB-ITSEF musi wdrożyć niezbędne i odpowiednie środki techniczne i organizacyjne w celu zapewnienia poufności wszystkich informacji uzyskanych lub wytworzonych w trakcie wykonywania działań certyfikacyjnych, w tym informacji dotyczących praw własności intelektualnej. Środki te muszą mieć zastosowanie do całego personelu oraz innych osób, którym przyznano dostęp do takich informacji. Certyfikacja systemu zarządzania bezpieczeństwem informacji CAB-ITSEF, której zakres obejmuje działalność laboratoryjną, jest uznawana za wystarczającą do spełnienia tego wymagania.

215 17025-01 GP-02: Rozszerzenia PN-EN ISO/IEC 17025 właściwe dla programu certyfikacji EUCC mają zastosowanie z ograniczeniem do obszaru kompetencji „oprogramowanie ogólne i urządzenia sieciowe”.

216 17025-02 GP-01/GP-02: Zarządzanie kompetencjami personelu musi być zgodne z PN-EN ISO/IEC 19896-1.

10 Okres przejściowy

217 W kontekście procesu akredytacji, CAB-CB może — pod nadzorem NAB i Właściciela programu — angażować się w wymagane działania certyfikacyjne, które powinny być obserwowane przez NAB.

218 W kontekście akredytacji CAB-ITSEF może – pod nadzorem NAB i Właściciela programu — angażować się w wymagane działania badania zgodności oraz ewaluacji cyberbezpieczeństwa, które powinny być obserwowane przez NAB. Sporządzenie raportów z badań i ewaluacji wymaga, aby CAB-ITSEF była akredytowana.

219 Wydanie certyfikatów po pomyślnym wykonaniu wszystkich działań w obszarze oceny i certyfikacji wymaga, aby CAB-CB była akredytowana.

220 Wnioskodawca oraz wszystkie strony zaangażowane w te działania muszą być w pełni świadome ich statusu i akceptować ryzyka związane z

możliwością, że CAB-CB lub CAB-ITSEF ostatecznie nie uzyskają akredytacji.

Załącznik A. Wymagania kompetencyjne dla rozwiązania Portfela EUDI

A.1 Zasady fundamentalne

221 *UWAGA: Wszystkie wymagania mają zastosowanie zarówno do CAB-CB, jak i CAB-ITSEF, o ile nie stwierdzono inaczej.*

222 CAB musi wykazać zdolność do prowadzenia certyfikacji na poziomie systemowym na podstawie heterogenicznych danych wejściowych dotyczących uzasadnienia zaufania, bez ponownego certyfikowania komponentów. Obejmuje to:

- o integrowanie zewnętrznych certyfikacji, raportów z badań i artefaktów uzasadnienia zaufania w spójny osąd na poziomie systemowym,
- o stosowanie rozumowania opartego na ryzyku tam, gdzie uzasadnienie zaufania jest częściowe, pośrednie lub odziedziczone,
- o zapewnianie identyfikowalności pomiędzy wymaganiami systemowymi a dowodami je wspierającymi, niezależnie od ich pochodzenia.

223 Wymaganie to NIE ma zastosowania do CAB-ITSEF.

A.2 Ramy kompetencji

A.2.1. Interpretacja certyfikacji zewnętrznych

224 CAB musi być w stanie:

- o oceniać zakres, poziom uzasadnienia zaufania i możliwość zastosowania certyfikacji stron trzecich,
- o interpretować zadania zabezpieczeń (Security Target), profile ochrony (Protection Profile) i raporty z certyfikacji,
- o identyfikować ograniczenia, założenia i ryzyka szczegółowe w ocenach zewnętrznych.

225 CAB-ITSEF musi być w stanie oceniać zadania zabezpieczeń i profile ochrony.

A.2.2. Kompetencje w zakresie kompozycji i integracji uzasadnienia zaufania

A.2.2.1. Integracja dowodów

226 CAB musi:

- o łączyć heterogeniczne artefakty uzasadnienia zaufania (certyfikacje, wyniki badań, raporty z audytów) w jednolitą ocenę,
- o zapewniać spójność pomiędzy różnymi źródłami uzasadnienia zaufania.

A.2.2.2. Analiza zależności i zaufania

227 CAB-CB musi:

- o identyfikować zależności zaufania pomiędzy komponentami i usługami,
- o oceniać, czy założenia przyjęte w certyfikacji jednego komponentu pozostają ważne w systemie złożonym.

A.2.2.3. Zarządzanie ryzykiem kompozycji

228 CAB musi:

- o oceniać ryzyka emergentne wynikające z interakcji komponentów,
- o walidować, że interfejsy i integracje nie unieważniają istniejących uzasadnień zaufania.

A.2.3. Mapowanie regulacyjne i analiza pokrycia

A.2.3.1. Identyfikowalność wymagań

229 CAB musi:

- o mapować wymagania europejskiego portfela tożsamości na dostępne dowody uzasadnienia zaufania,
- o utrzymywać dwukierunkową identyfikowalność pomiędzy wymaganiami a wykazaniem zgodności komponentów i usług.

A.2.3.2. Identyfikacja i obsługa luk

230 CAB musi:

- o identyfikować luki pokrycia w certyfikacjach zewnętrznych lub dowodach uzasadnienia zaufania,
- o definiować zabezpieczenia kompensujące, dodatkowe dowody lub ukierunkowane oceny.

A.2.4. Techniczne kompetencje w zakresie cyberbezpieczeństwa

A.2.4.1. Ocena dowodów technicznych

231 CAB musi być zdolna do:

- o oceny architektury systemu i granic zaufania,
- o oceny praktyk bezpiecznego projektowania i implementacji,
- o przeprowadzania ocen podatności oraz oceny wyników testów penetracyjnych,
- o przeprowadzania oceny SZBI (ISMS).

232 CAB-ITSEF musi być zdolna do przeprowadzania oceny podatności oraz projektowania i przeprowadzania testów penetracyjnych.

A.2.4.2. Wiedza ekspercka w zakresie kryptografii i usług zaufania

233 CAB musi:

- o rozumieć mechanizmy kryptograficzne i zarządzanie kluczami,
- o oceniać odporność na zaawansowane scenariusze ataków (np. wysoki potencjał ataku),
- o oceniać mechanizmy bezpiecznej komunikacji i wiązania tożsamości

234 CAB-ITSEF musi być zdolna do przeprowadzania oceny mechanizmów kryptograficznych i zarządzania kluczami.

A.2.5. Uzasadnienie zaufania w cyklu życia i łańcuchu dostaw

A.2.5.1. Ocena bezpiecznego cyklu życia

235 CAB musi oceniać:

- o procesy rozwoju, integracji, wdrażania i utrzymania,
- o obsługę podatności, mechanizmy bezpiecznej aktualizacji i zarządzania poprawkami.

A.2.5.2. Ryzyko łańcucha dostaw i stron trzecich

236 CAB musi:

- o oceniać wiarygodność dostawców i ryzyka zależności,

- o weryfikować integralność procesów wytwarzania, zasilania (provisioning) i dystrybucji.

A.2.6. Ocena usług ICT i bezpieczeństwa operacyjnego

A.2.6.1. Uzasadnienie zaufania na poziomie usług

237 CAB musi:

- o oceniać ewaluację środowisk operacyjnych wspierających portfel,
- o oceniać integrację tożsamości, uwierzytelniania i usług zaufania.

A.2.6.2. Systemy zarządzania i zgodność

238 CAB musi być kompetentna w ocenie:

- o systemów zarządzania bezpieczeństwem informacji zgodnych z normami takimi jak EN PN-EN ISO/IEC 27001, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, CIS Critical Security Controls, właściwe normy ETSI,
- o ram regulacyjnych obejmujących dyrektywę NIS 2.

A.2.7. Raportowanie, identyfikowalność i uzasadnianie

A.2.7.1. Raportowanie ustrukturyzowane

239 CAB musi:

- o wytwarzać jasne, ustrukturyzowane i audytowalne raporty z oceny,
- o zapewniać identyfikowalność od ustaleń do dowodów i wymagań.

240 CAB-ITSEF musi wytwarzać jasne, ustrukturyzowane i identyfikowalne raporty techniczne oparte na powiązaniu ustaleń z dowodami i wymaganiami.

A.2.7.2. Uzasadnianie decyzji certyfikacyjnych

241 CAB musi:

- o jasno uzasadniać, w jaki sposób dowody zewnętrzne wspierają twierdzenia certyfikacyjne,
- o jawnie dokumentować założenia, ograniczenia i ryzyka szczątkowe.

A.2.8. Niezależność, bezstronność i ład organizacyjny

A.2.8.1. Bezstronne wykorzystywanie dowodów zewnętrznych

242 CAB musi:

- o oceniać dowody stron trzecich bez nadmiernego polegania na nich ani stronniczości,
- o utrzymywać niezależność od deweloperów komponentów oraz certyfikujących lub oceniających, w stosownych przypadkach.

A.2.9. Koordynacja interesariuszy i świadomość ekosystemu

A.2.9.1. Koordynacja wielostronna

243 CAB musi skutecznie współdziałać z:

- o dostawcami portfela,
- o jednostkami certyfikującymi lub laboratoriami badawczymi stron trzecich,
- o organami krajowymi (np. organami certyfikacji cyberbezpieczeństwa)

A.2.9.2. Obsługa podatności i incydentów

244 CAB musi:

- o weryfikować procesy ujawniania i usuwania podatności,
- o zapewniać zgodność z praktykami skoordynowanego ujawniania podatności.

245 Wymaganie to ma zastosowanie do programów certyfikacji GP-02 i GP-03.

A.2.10. Ciągłe uzasadnienie zaufania i działania po certyfikacji

A.2.10.1. Bieżąca zgodność

246 CAB-CB musi:

- o stosować zdefiniowane mechanizmy nadzoru, ponownej oceny i zarządzania zmianami

247 CAB-ITSEF musi współpracować z CAB-CB w działaniach po certyfikacji.

A.2.10.2. Ryzyko szczątkowe i monitorowanie

248 CAB-CB musi:

- o oceniać i dokumentować ryzyka szczątkowe na poziomie Portfela EUDI oraz dokumentować wynik oceny

- o rekomendować strategię monitorowania i łagodzenia ryzyka.

249

Wymaganie to NIE ma zastosowania do CAB-ITSEF.