INFORMATOR DLA KLIENTÓW

Jednostki Certyfikującej NASK

Certyfikat Common Criteria

na zasadach określonych przez:

Program oceny i certyfikacji bezpieczeństwa IT

NASK

SPIS TREŚCI

1. Cel dokumentu

Celem dokumentu jest wstępne przybliżenie istoty standardu Common Criteria jako narzędzia oceny bezpieczeństwa produktów teleinformatycznych oraz podstaw certyfikacji wyrobów (produktów).

2. Zakres dokumentu

Dokument jest sformułowany w postaci listy pytań i odpowiedzi na nie. Wyselekcjonowano pytania, które mogą nasunąć się zarówno niedoświadczonemu użytkownikowi standardu Common Criteria, jak również osobie zainteresowanej zgłębieniem tematu certyfikacji cyberbezpieczeństwa.

3. Odbiorcy dokumentu

1. Klienci zainteresowani certyfikacją swoich produktów.
2. Kupujący zainteresowani rozpoznawaniem certyfikatów w specyfikacjach przedmiotu zamówienia.
3. Laboratoria zainteresowane wykonywaniem badań.

4. Dokumenty referencyjne i system pojęć

- **CC** – Common Criteria for Information Technology Security Evaluation:

  Part 1: Introduction and general model (ISO/IEC 15408-1)

  Part 2: Security functional requirements (ISO/IEC 15408-2)

  Part 3: Security assurance requirements (ISO/IEC 15408-3)

- norma **PN EN ISO/IEC 15408** dotycząca certyfikacji produktów teleinformatyki – ekwiwalent standardu CC tj. np. PN EN ISO/IEC 15408-1:2020-09 odpowiada Part 1 Common Criteria

- norma **PN EN ISO/IEC 18045** dotycząca metodyki ewaluacji cyberbezpieczeństwa produktów IT – ekwiwalent standardu CEM

- **EAL** – Evaluation Assurance Level – poziom uzasadnienia zaufania (do zabezpieczeń) od EAL 1 do EAL 7;

- **PP** – Protection Profile (Profil Zabezpieczeń) – dokument określający wymagania względem bezpieczeństwa przynależące danej grupie produktowej (np. urządzeń sieciowych, syste-mów operacyjnych, tachografów, modułów kryptograficznych, etc.);

- **cPP** – collaboration Protection Profile - dokument określający wymagania względem bezpieczeństwa przynależące danej grupie produktowej stworzony przez oficjalną grupę roboczą (CC Working Group);

- **ST** – Security Target, Specyfikacja Zabezpieczeń – dokument określający realizację wymogów bezpieczeństwa produktu podlegającego certy-fikacji;

- **TOE** – Target Of Evaluation – produkt podlegający ocenie.

5. Czym jest standard Common Criteria (CC)?

Common Criteria (CC) to międzynarodowy standard (dostępny jako norma PN-EN ISO/IEC 15408) służący ocenie właściwości bezpieczeństwa produktów i systemów IT. Standard określa wymogi bezpieczeństwa oraz metodologię dokumentowania zabezpieczeń. Standard CC jest wykorzystywany przez rządy i organizacje prywatne na całym świecie do oceny bezpieczeństwa produktów technologii informatycznych, a zgodność z normą jest często wymagana jako warunek konieczny do podjęcia współpracy.

Więcej informacji na temat standardu Common Criteria oraz treść dokumentów **CC** i **CEM** można znaleźć na stronie commoncriteriaportal.org

6. Kto honoruje certyfikaty CC?

Obecnie certyfikaty CC są uznawane przez następujące państwa: Australia, Austria, Belgia, Chorwacja, Czechy, Dania, Estonia, Etiopia, Finlandia, Francja, Niemcy, Grecja, Hiszpania, Indie, Indonezja, Izrael, Japonia, Kanada, Katar, Republika Korei, Luksemburg, Malezja, Holandia, Nowa Zelandia, Norwegia, Pakistan, Polska, Singapur, Słowacja, Stany Zjednoczone, Szwecja, Turcja, Węgry, Wielka Brytania, Włochy.

Aktualna lista krajów uczestniczących znajduje się na stronie commoncriteriaportal.org.

Inne państwa i organizacje mogą również korzystać z certyfikatów **CC**, każdy w swoim zakresie i zgodnie z wewnętrznymi regulacjami. Przykładem organizacji stosującej certyfikaty Common Criteria we własnych procedurach kontraktacji jest **NATO**.

Kraje wykorzystujące certyfikację zgodną z CC zrzeszone są w dwóch organizacjach:

- SOG-IS – Senior Officials Group Information Systems Security jest porozumieniem zrzeszającym kraje europejskie (obecnie 17) w oparciu o SOG-IS Mutual Recognition Agreement (SOG-IS MRA). Dokument ten określa warunki wzajemnego honorowania certyfikatów przez kraje członkowskie. Wszystkie certyfikaty do poziomu EAL4 są wzajemnie rozpoznawane przez strony porozumienia. Ponadto w dwóch wyspecyfikowanych dziedzinach:„smart card” i „security boxes” certyfikaty honorowane są do najwyższego poziomu EAL7. Więcej: sogis.eu/index_en.html

– CCRA – Common Criteria Recognition Arrangement jest organizacją zrzeszającą 31 krajów z 4 kontynentów. W oparciu o Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security strony porozumienia wzajemnie honorują certyfikaty do poziomu EAL2. Ponadto w przypadku certyfikowania produktu względem wspólnie wypracowanego Profilu Zabezpieczeń (collaboration Protection Profile - cPP), rozpoznawane są certyfikaty do poziomu EAL4. Więcej: https://www.commoncriteriaportal.org/ccra/index.cfm

7. Jakie strony uczestniczą w postępowaniu certyfikującym wg standardu CC?

W procesie oceny CC zaangażowane są trzy strony:

1. **Klient** (producent, rzadziej dostawca), który przedstawia do oceny swój Produkt do Oceny (TOE - Target Of Evaluation) oraz związany z nim materiał dowodowy;
2. **Laboratorium**, które przeprowadza ocenę i tworzy sprawozdanie z badań. Laboratorium, które przeprowadza ocenę i tworzy sprawozdanie z badań. Ocena ma charakter iteracyjny, a producent/sponsor może odnieść sie do ustaleń powstałych w trakcie jej procesu;
3. **Jednostka Certyfikująca**, czyli instytucja wydająca certyfikaty CC i sprawująca nadzór nad Laboratoriami. Każda Jednostka Certyfikująca ma swój własny Program Certyfikacji określający sposób stosowania CC w danym kraju i ograniczenia typu produktów, które mogą podlegać ocenie. W Polsce uruchomiono jedną Jednostkę Certyfikującą (NASK) oraz dwa Laboratoria świadczące usługi ewaluacji cyberbezpieczeństwa produktów IT. NASK opracował, wdrożył i stosuje Program Certyfikacji pn. „PC1 – Program oceny i certyfikacji bezpieczeństwa IT".

8. Jaki jest zakres oceny produktu?

Zbiór czynności w ocenie produktu jest zależny od wymagań uzasadnienia zaufania zawartych w dokumencie Specyfikacji Zabezpieczeń (ST, Security Target).

Poniżej przedstawiono przegląd głównych etapów oceny:

– ***Specyfikacja Zabezpieczeń (ST – Security Target)*** – dokument deklaratywny, który określa funkcje bezpieczeństwa podlegające ocenie oraz elementy uzasadnionego zaufania do zabezpieczeń, jakie spełnia produkt;

– ***Profil zabezpieczeń (PP - Protection Profile)*** – dokument określający potrzeby bezpieczeństwa dla danej klasy produktów;

– ***Ocena dokumentacji technicznej*** – ocena dokumentacji produktu dokonywana z rosnącą szczegółowością, w zależności od rygoru certyfikatu (tzw. poziomy wnikliwości oceny EAL1 do EAL7). Proces oceny dokumentacji oznacza szczegółową

Rys. 1 Symboliczne przedstawienie członków obu porozumień

analizę specyfikacji projektu produktu, włącznie z detalami architektury rozwiązania, a nawet przeglądem kodu źródłowego. O szczegółowości oceny decydują wymagania bezpieczeństwa określone w dokumentach kryterialnych (standardzie) dla danego poziomu EAL;

- ***Ocena dokumentacji użytkownika*** - ocena wszystkich dostarczonych dokumentów zawie-rających wytyczne użytkowania produktu w konfiguracji będącej przedmiotem certyfikacji wraz z „Przewodnikiem bezpiecznej instalacji";
- ***Ocena cyklu życia*** - ocena praktyk zarządzania konfiguracją, procedur dostarczania oraz śledzenia błędów bezpieczeństwa (problemów użytkowania). Ocena może również obejmować metody programistyczne i audyty bezpieczeństwa środowiska użytkowania produktu;
- ***Testy funkcjonalności*** - osoby przeprowadzające ocenę zgodności powtarzają przykładowe, funkcjonalne testy wykonane przez programistów oraz przeprowadzają własne, niezależne testy, aby potwierdzić skuteczne działanie wyspecyfikowanych funkcji bezpieczeństwa;
- ***Testy penetracyjne*** - osoby przeprowadzające ocenę zgodności przeprowadzają analizę podatności na zagrożenia i przeprowadzają testy penetracyjne.

9. Czym jest Specyfikacja Zabezpieczeń (ST – Security Target)?

Specyfikacja Zabezpieczeń to dokument definiujący produkt do oceny (TOE – Target Of Evaluation), czyli produkt, konfigurację i wersję oraz zakres funkcji bezpieczeństwa podlegających ocenie.

Według standardu CC, przedmiotem oceny (TOE) może być cały lub część produktu lub systemu.

Specyfikacja Zabezpieczeń jest tworzona przy użyciu elementów standardu CC i obejmuje model zagrożenia, założenia środowiskowe, cele bezpieczeństwa, wymagania funkcjonalne zabezpieczeń (SFR – Security Functional Requirements) oraz wymogi uzasadnionego zaufania do zabezpieczeń (SARs – Security Assurance Requirements). Specyfikacja może być oparta na tzw. Profilu Zabezpieczeń (Protection Profile) dla danego typu rozwiązań, aczkolwiek nie jest to konieczne. Specyfikacja zabezpieczeń (ogólnie: napisany przez producenta) wykraczająca poza Profil Zabezpieczeń (ogólnie: napisany przez konsumenta), wymaga dołączenia dodatkowego opisu o sposobie osiągnięcia przez produkt określonych wymagań bezpieczeństwa.

Przykłady ST można znaleźć na stronie: Certified Products : CC Portal (commoncriteriaportal.org)

10. Czym jest Profil Zabezpieczeń (PP – Protection Profile)?

Profil Zabezpieczeń jest dokumentem formułującym wymagania bezpieczeństwa dla wybranego typu produktów w oparciu o standard Common Criteria.

Profile Zabezpieczeń są publikowane m. in. przez rządy w odniesieniu do określonego rodzaju technologii, na przykład zapory systemowe, również jako część polityki zamówień publicznych (public procurement).

Profil zabezpieczeń określa zarówno wymagania dotyczące funkcjonalności, jak i uzasadnionego zaufania. Nie jest konieczne, aby specyfikacja zabezpieczeń była zawsze tworzona w oparciu o profil zabezpieczeń, jednak niektóre jednostki certyfikujące będą przyjmowały do oceny tylko te produkty, które potwierdzają zgodność z profilami zabezpieczeń zatwierdzonymi przez jednostkę certyfikującą. Dany produkt może być zgodny z wieloma profilami zabezpieczeń.

Repozytorium profili zabezpieczeń jest publikowane na stronie: Collaborative Protection Profiles (cPP) and Supporting Documents (SD) : CC Portal (commoncriteriaportal.org)

11. Czym jest Collaborative Protection Profile (cPP)?

Collaboration Protection Profile jest profilem zabezpieczeń wypracowanym w ramach współpracy różnych środowisk zainteresowanych stworzeniem wspólnego standardu wymagań bezpieczeństwa dla danej grupy produktowej, np. producentów kart inteligentnych (smart cards). Więcej informacji dotyczących tej inicjatywy można znaleźć na stronie commoncriteriaportal.org/communities/technical_communities.cfm

12. Czym jest poziom uzasadnienia zaufania (EAL – Evaluation Assurance Level)?

EAL jest zdefiniowanym zbiorem wymagań uzasadniających zaufanie do produktu. Najmniej rygorystycznym (najniższym) poziomem jest EAL1 (testowanie funkcjonalne), a najbardziej rygorystycznym (najwyższym) jest poziom EAL7.

Profil Zabezpieczeń (PP) lub Specyfikacja Zabezpieczeń (ST) może określać zgodność z danym poziomem bezpieczeństwa EAL lub definiować własny zestaw wymagań uzasadniających zaufanie.

13. Jak długo trwa proces certyfikacji?

Proces oceny i certyfikacji trwa na świecie średnio około roku. Czas trwania zależy od wielu czynników, z których najważniejszymi są złożoność produktu podlegającego ocenie i deklarowany poziom uzasadnienia zaufania (EAL).

Przeprowadzenie oceny wiąże się z przygotowaniem produktu (zgodnie ze standardem CC), przygotowaniem niezbędnej dokumentacji, przekazaniem do ewaluacji akredytowanemu Laboratorium oraz oceny zgodności i wydaniem ostatecznego certyfikatu przez akredytowaną Jednostkę Certyfikującą.

14. Co się dzieje, kiedy certyfikowany produkt ulega modyfikacji?

Certyfikat standardu Common Criteria dotyczy produktu w konfiguracji i wersji zadeklarowanej w danej Specyfikacji Zabezpieczeń (ST).

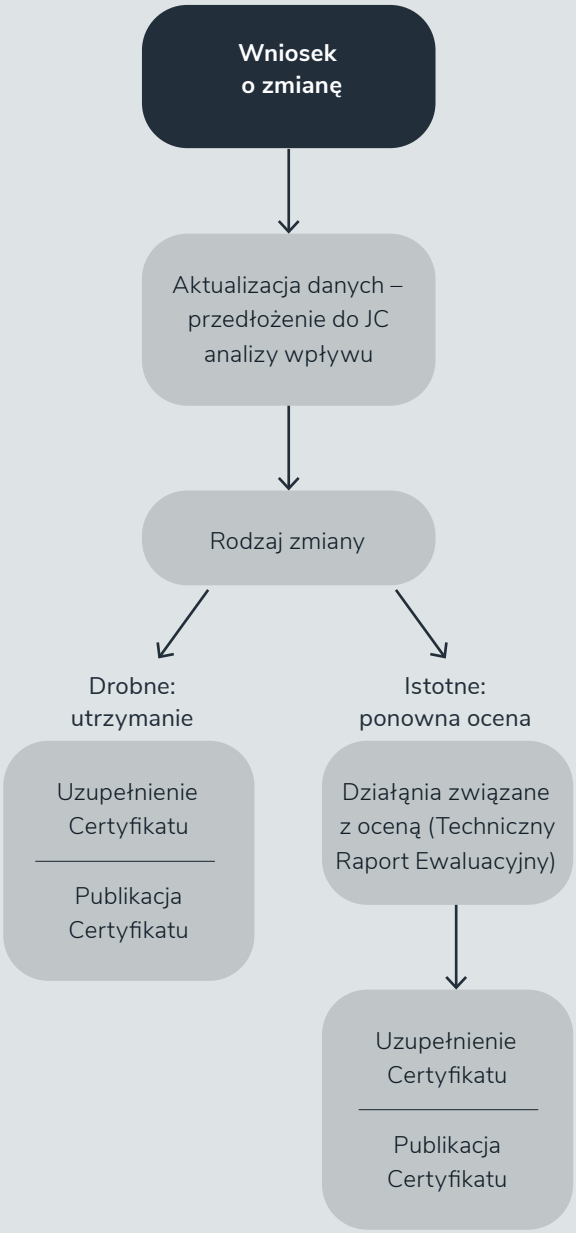
Dla przykładu, jeśli certyfikowano produkt w wersji v 1.0, uaktualniona wersja v1.0.1 nie posiada statusu produktu certyfikowanego. W przypadku nieznacznych zmian produktu certyfikowanego dostępna jest uproszczona ścieżka służąca uaktualnieniu certyfikatu, zwana **Utrzymaniem Zaufania (AC – Assurance Continuity).** Jednostka Certyfikująca NASK-PIB, na wniosek Klienta przeprowadza weryfikację wydanego certyfikatu w oparciu o wewnętrzną instrukcję I29/2.1

15. Jak działa weryfikacja zakresu certyfikatu i ‘Utrzymanie Zaufania’ (AC – Assurance Continuity)?

Utrzymanie Zaufania jest procesem zapewniającym możliwość rozszerzenia certyfikatu na produkt uprzednio certyfikowany, którego wersja lub konfiguracja została zaktualizowana (produkt uległ modyfikacji, przez co utracił status produktu certyfikowanego).

W przypadku gdy zmiany produktu dotyczą zagadnień bezpieczeństwa (klasyfikowanych jako „ważne”), procedura pozwala na szybką ocenę tychże w ramach tzw. recertyfikacji, korzystającej z informacji pochodzących z uprzednio przeprowadzonego procesu certyfikacji.

UWAGA: poszczególne jednostki certyfikujące same określają politykę dotyczącą ścieżki przeprowadzania procesu AC. W przypadku NASK-PIB zachowana jest zgodność z wytycznymi CCRA, co szczegółowo opisano w dokumencie: ***Assurance Continuity*** oraz wewnętrznej instrukcji Jednostki Certyfikującej pn. „I29/2.1---PL_Instrukcja_weryfikacji_zakresu certyfikatu-EN_Certificate_scope_verification”.



Rys.2 Podstawowy schemat weryfikacji zakresu certyfikatu.

16. Dlaczego warto korzystać z produktów certyfikowanych według standardu CC?

Produkty posiadające certyfikat zgodności ze standardem CC zostały poddane rygorystycznemu procesowi oceny, który został przeprowadzony na podstawie ewaluacji cyberbezpieczeństwa, wykonanej przez niezależne Laboratoria, według międzynarodowego standardu (kryteriów) w ramach Programu Certyfikacji ustanowionego przez Jednostkę Certyfikującą.

Korzystanie z certyfikowanych produktów, wiąże się z następującymi korzyściami:

- funkcje bezpieczeństwa zostały przetestowane i potwierdzone;
- produkt przeszedł badania w zakresie podatności na zagrożenia i testy penetracyjne;
- przeprowadzono ocenę procesu tworzenia produktu;
- spełnione są wymogi standardu CC w kontekście procesu dostarczania i uruchamiania produktu.

17. Dlaczego warto certyfikować swój produkt według standardu CC?

Korzyści wynikające z przeprowadzenia procesu certyfikacji produktu (poza wymienionymi w punkcie 16):

- w wielu krajach certyfikat jest potwierdzeniem spełnienia wymagań stawianych w specyfikacji zamówień dla przemysłu i administracji publicznej;
- prowadzi do doskonalenia produktu i procesu wytwarzania dzięki spostrzeżeniom poczynionym na etapie oceny;
- umożliwia uzyskanie certyfikatu honorowanego (rozpoznawanego) przez kraje zrzeszone w ramach porozumienia CCRA (Świat) i SOG-IS (Europa);
- zapewnia lepszą pozycję konkurencyjną w obrocie rynkowym.

18. Jak przygotować produkt do certyfikacji?

1. Odwiedź stronę commoncriteriaportal.org
2. Zapoznaj się ze standardem Common Criteria (trzy części) oraz standardem oceny Common Evaluation Methodolgy, Common Criteria : CC Portal (commoncriteriaportal.org)
3. Poszukaj podobnego do Twojego produktu na liście certyfikowanych produktów i przeczytaj jego dokumentację dostępną publicznie (w szczególności Security Target): Certified Products : CC Portal (commoncriteriaportal.org)
4. Poszukaj czy istnieje Protection Profile do typu produktów mających zastosowanie dla Twojego produktu:

- Protection Profiles : CC Portal (commoncriteriaportal.org)
- sogis.eu/uk/pp_en.html

5. Przeczytaj jak zebrać materiał dowodowy, potrzebny do oceny produktu (Collection of Developer Evidence; sogis.eu/documents/cc/common/JIL-Collection-of-Developer-Evidence-v1-5.pdf)
6. Zapisz się do Forum Użytkowników CC (CCUF) tj. społeczności standardu CC obejmującej dostawców, doradców, laboratoria testowe, komitety organizacyjne CC, narodowe centra certyfikujące, twórców programów certyfikacji i innych podmiotów zainteresowanych standardem.
7. Zapoznaj się z przewodnikiem w zakresie tworzenia materiału dowodowego: Guidelines for Developer Documentation przygotowanym przez niemiecką Jednostkę Certyfikującą tj. Bundesamt für Sicherheit in der Informationstechnik commoncriteriaportal.org/files/ccfiles/CommonCriteriaDevelopersGuide_1_0.pdf
8. Wybierz Laboratorium, które udzieli Ci wsparcia:

- w Polsce: https://certyfikacja.nask.pl/laboratoria/
- w Europie: sogis.eu/uk/status_participant_en.html
- na świecie: https://www.commoncriteriaportal.org/labs/index.cfm

Wyślij wniosek do Jednostki Certyfikującej NASK -PIB: https://certyfikacja.nask.pl/kontakt/

9. Zbierz niezbędne dowody, we współpracy z Laboratorium, przejdź przez proces ewaluacji cyberbezpieczeństwa. Dowody zebrane i dostarczone do Jednostki Certyfikującej zostaną poddane ocenie, a w przypadku potwierdzenia zgodności z wymaganiami zapadnie pozytywna decyzja o wydaniu certyfikatu. W ten sposób uzyskasz **Certyfikat Common Criteria**.

19. Jakie są opłaty, którymi są obciążani wnioskujący i klienci?

NASK-PIB jest państwowym instytutem badawczym nadzorowanym przez Kancelarię Ministra, finansowanym ze środków:

- dotacji naukowej;
- publicznych, przeznaczonych na realizacje zadań publicznych;
- zewnętrznych przeznaczonych na realizacje projektów dofinansowanych;

– pochodzących z komercyjnej działalności, z zachowaniem bezstronności Jednostki Certy-fikującej.

Obszary działalności oraz aktywności Instytutu są szczegółowo opisane na stronie internetowej NASK w zakładce „Działalność" oraz „Projekty dofinansowane".

Klienci wnioskujący o certyfikację są obciążani opłatami w wysokości umownej zależnej od poziomu komplikacji danego procesu certyfikacji.

Opłaty można podzielić na następujące grupy:

– opłata za rozpatrzenie wniosku; opłata w stałej wysokości, jednorazowa, bezzwrotna;

– opłata za proces certyfikacji – zależna od nakładu prac; obliczana na podstawie szacowanego zaangażowania pracowników dla danego typu produktu IT i poziomu EAL; rozliczana etapami;

– opłata po wydaniu certyfikatu – za czynności wykonywane przez Jednostkę Certyfikującą w ramach nadzoru nad wykorzystaniem certyfikatu; opłata pobierana jest z góry za każdy rok ważności certyfikatu.

Dodatkowym kosztem, który obciąża klienta w procesie certyfikacji jest opłata za prace Laboratorium wykonującego ewaluację cyberbezpieczeństwa – zgodnie z umową Klienta z Laboratorium. Jednostka Certyfikująca nie uczestniczy ani nie pośredniczy w zawieraniu umowy pomiędzy Laboratorium a Klientem.

20. Jakie są prawa i obowiązki wnioskujących i klienów?

Klient ma prawo do certyfikacji prowadzonej na zasadach równych dla wszystkich wnioskujących, prowadzonej rzetelnie i bezstronnie zgodnie z przyjętą przez NASK-PIB polityką opisaną w dokumencie „PT10 – Polityka jakości, bezstronności i poufności Jednostki Certyfikującej".

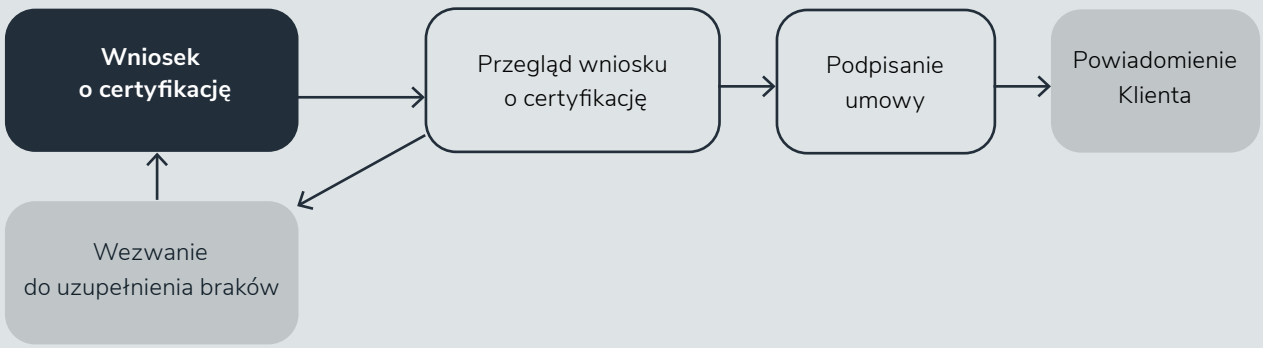
Klient ma obowiązek wypełniać wymogi certyfikacyjne określone w Programie Certyfikacji oraz szczegółowo zdefiniowane w Umowie i Kontrakcie.

Wzór wniosku certyfikacyjnego, wzór oświadczenia o spełnianiu wymagań, wzór umowy o świadczenie usługi, Program Certyfikacji oraz wzór kontraktu są dostępne na życzenie.

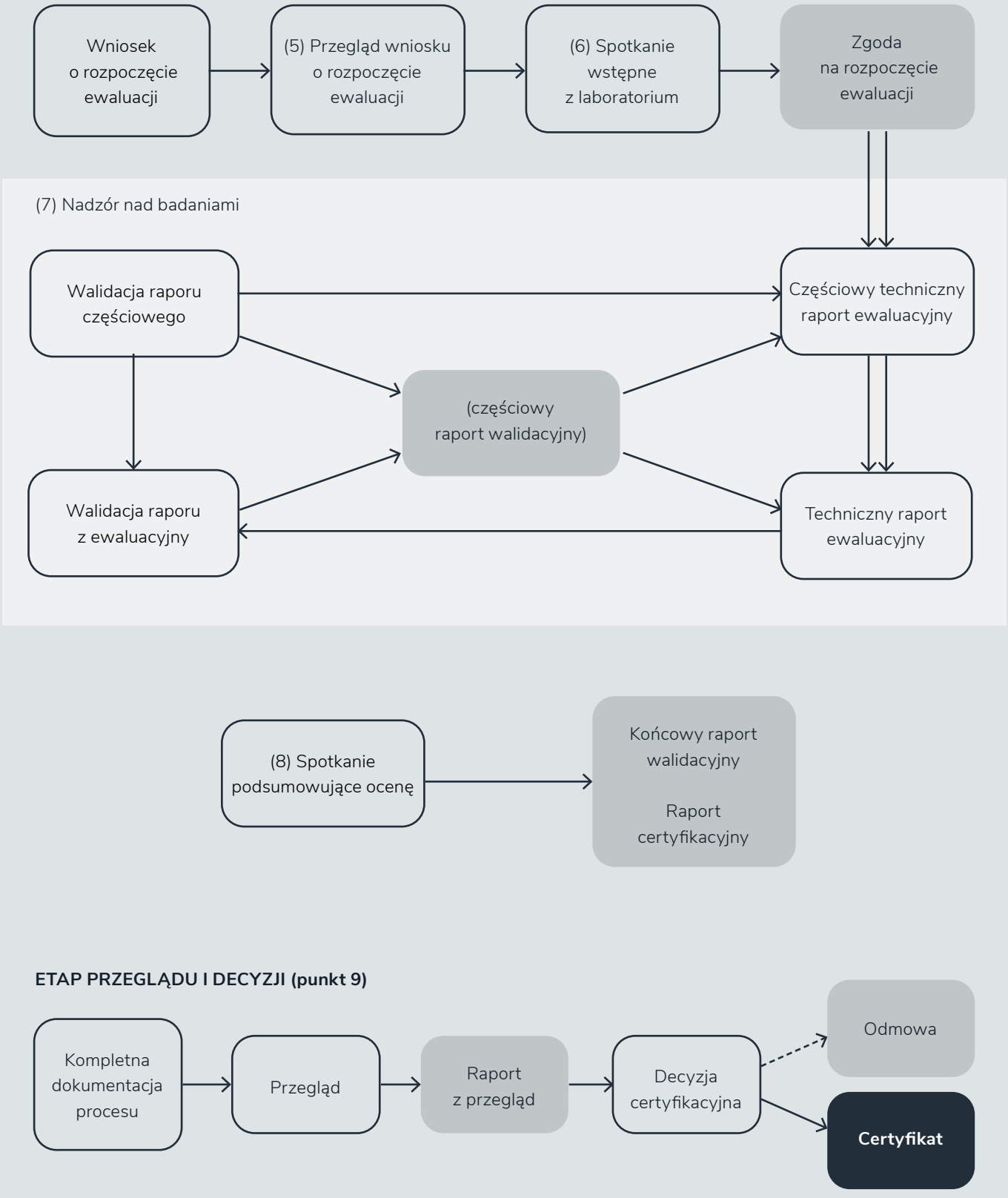
21. Jakie są zasady wydawania certyfikatu?

Wymagania certyfikacyjne i szczegółowy przebieg certyfikacji opisuje dokument „PC1 – Program oceny i certyfikacji bezpieczeństwa IT" oraz dokument „P33 – Certyfikacja Produktu" (patrz: Diagram „Schemat postępowania w procesie certyfikacji" na następnej stronie). Oba dokumenty dostępne są na życzenie dla przyszłych Klientów Jednostki Certyfikującej (patrz: sekcja 'Kontakt' na końcu dokumentu).

ETAP PRZEGLĄDU WNIOSKU (punkt 4)



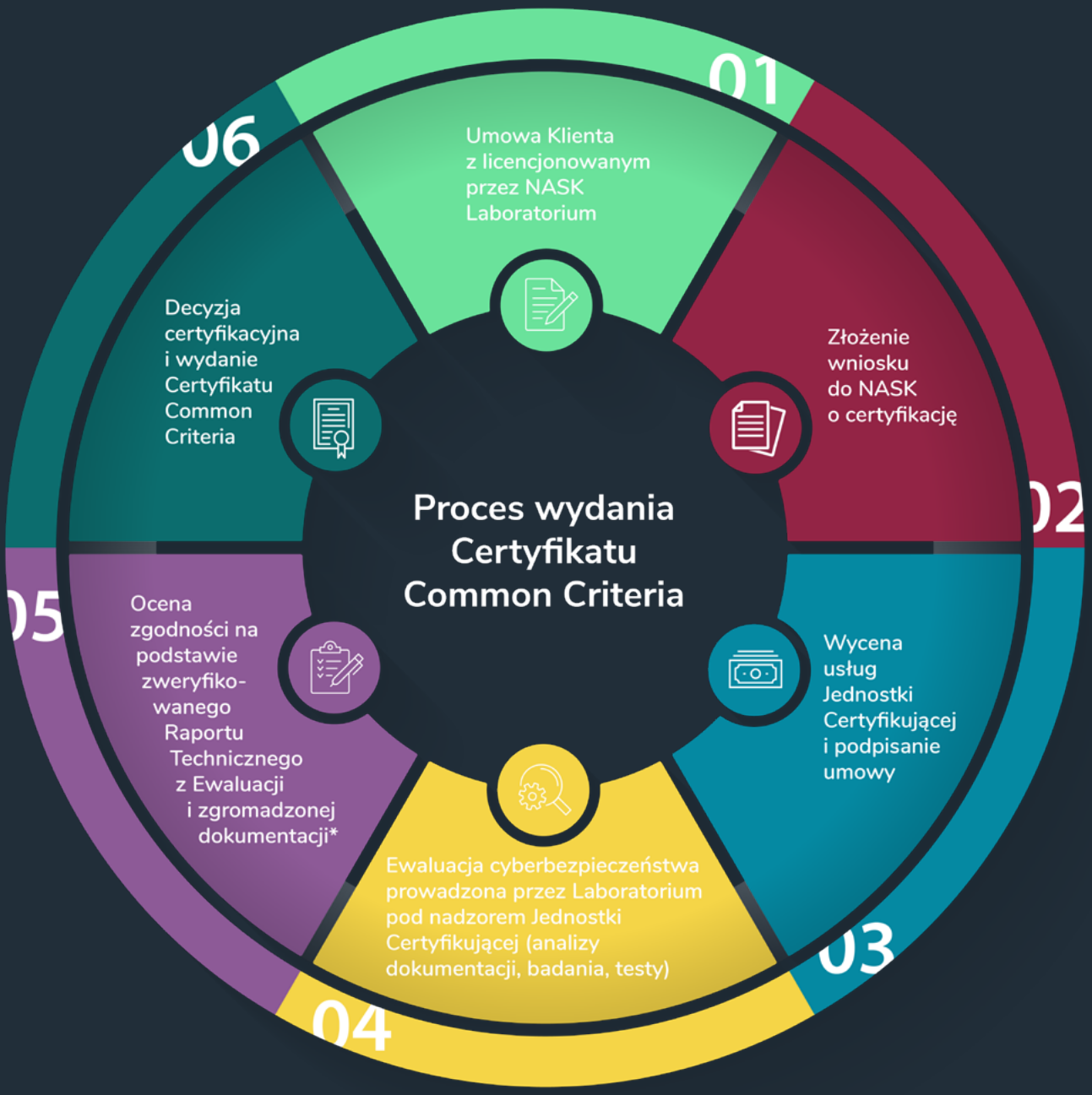
ETAP OCENY (punkt 5-8)



ETAP PRZEGLĄDU I DECYZJI (punkt 9)

Rys.3 Podstawowy schemat postępowania w procesie certyfikacji.

22. Na skróty: jak otrzymać certyfikat?



*w przypadku stwierdzenia niezgodności przedmiotu oceny (produktu) z wymaganiami Klient jest o tym informowany i uzgadniane jest dalsze postępowanie (np. ponowna ocena)

Jednostka Certyfikująca
Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy

ul. Kolska 12, 01-045 Warszawa

e-mail: standard@nask.pl, tel. +48 22 380 82 00

NASK-PC1 – Program oceny i certyfikacji bezpieczeństwa IT – informator dla Klientów