Streszczenie dokumentu polityki certyfikacji

Wersja: 2.3

Karta dokumentu:

Tytuł dokumentu	STRESZCZENIE DOKUMENTU POLITYKI CERTYFIKACJI CCK MF
Właściciel dokumentu	Departament Bezpieczeństwa Ministerstwa Finansów Rzeczypospolitej Polskiej
Wersja	2.3
Status dokumentu	**Zatwierdzony**
Data zatwierdzenia	11.05.2026
Ilość stron	8

zatwierdzony przez:

Wersja	Zatwierdzony przez
2.3	Dyrektor Departamentu Bezpieczeństwa Ministerstwa Finansów

Spis treści

1 Informacje kontaktowe

Punktem kontaktowym do załatwiania wszelkich spraw związanych z realizacją polityki certyfikacji przez Ministerstwo Finansów (dalej: **MF**) Rzeczypospolitej Polskiej jest:

Ministerstwo Finansów
Departament Bezpieczeństwa

Adres pocztowy, nazwiska kadry kierowniczej i telefon kontaktowy są publikowane na stronie internetowej:

https://www.gov.pl/web/finanse/departament-bezpieczenstwa

e-mail: sekretariat.dbe@mf.gov.pl

W ramach system certyfikacji CCK[1] MF (patrz rozdział **2.1**), certyfikaty publicznie dostępne wydawane są wyłącznie w ramach następujących podsystemów: *CCK MF Zewnętrzne* i *CCK KSeF*.

Wraz z certyfikatem podsystem *CCK MF Zewnętrzne* udostępnia subskrybentowi poufny kod identyfikacyjny, niezbędny do uwierzytelnienia w kontaktach z CCK MF, w tym przy unieważnianiu certyfikatu, zawieszaniu i uchylaniu zawieszenia.

Aby unieważnić certyfikat wydany na dany identyfikator w podsystemie *CCK KSeF* należy uwierzytelnić się środkiem uwierzytelnienia zawierającym ten identyfikator, tj. NIP lub PESEL, albo – w przypadku certyfikatu kwalifikowanego niezawierającego NIP lub PESEL – kwalifikowanym certyfikatem, którego skrót SHA256 (tzw. *odcisk palca*) znajduje się w unieważnianym certyfikacie.

Szczegóły właściwej procedury unieważniania certyfikatu można znaleźć w dokumentach publikowanych w języku polskim na stronach internetowych:

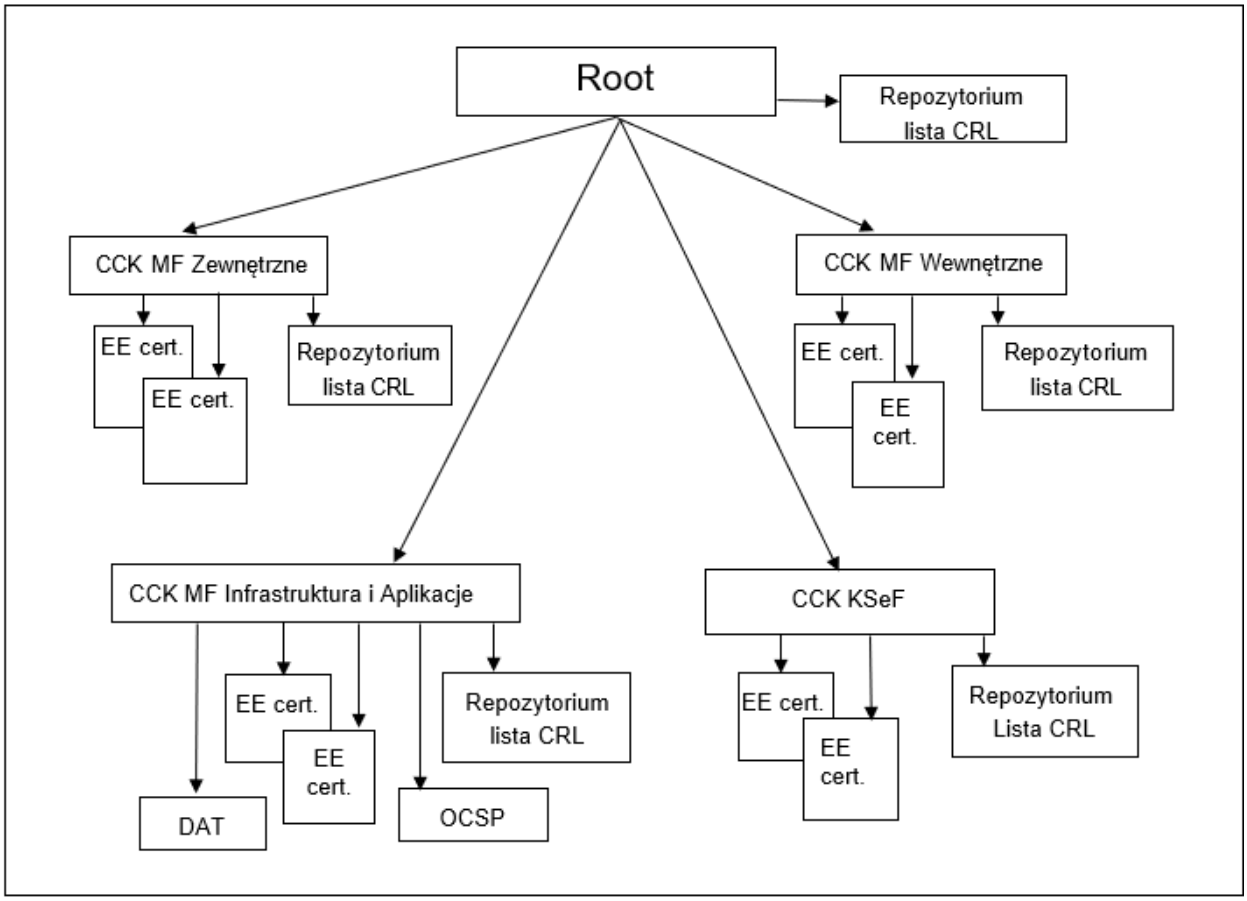
- w przypadku *CCK MF Zewnętrzne*
  https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny
- w przypadku *CCK KSeF*
  https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/

2 Rodzaje certyfikatów, procedury walidacji i użycie

2.1 Rodzaje certyfikatów

System certyfikacji „CCK MF" składa się z Root'a i podsystemów certyfikacji, jak pokazano na poniższym rysunku:

[1] *Centrum Certyfikacji*; inaczej: *CA* (ang. *Certification Authority*)



Rysunek 1 System PKI - schemat logiczny

Root wydaje tylko zaświadczenia certyfikacyjne (ang. *CA certificates*):

- samopodpisane zaświadczenie certyfikacyjne (ang. *self-signed certificates*) dla dystrybucji kotwicy zaufania,
- zaświadczenia certyfikacyjne (ang. *cross-certificates*) dla podrzędnych subCA.

Podrzędne subCA wydają tylko certyfikaty użytkowników końcowych (ang. *EE certificates*):

- certyfikaty subskrybentów,
- certyfikaty dla Respondera OCSP[2] (tylko subCA "Infrastruktura i Aplikacje").

Subskrybentem usług zaufania w ramach CCK MF może być każda osoba fizyczna posiadająca pełną zdolność prawną lub każda osoba prawna w rozumieniu prawa krajowego, a także każdy inny podmiot o podobnym charakterze (jednostka organizacyjna nieposiadająca osobowości prawnej, spółka cywilna itp.) lub – w przypadku subCA „Infrastruktura i Aplikacje" – nawet urządzenie lub aplikacja.

Wszystkie certyfikaty mają profil zgodny ze standardem X.509 v3.

Klucze prywatne do podpisów/pieczęci elektronicznych mogą być generowane i przechowywane na urządzeniach takich jak karty inteligentne, a także mogą być generowane w aplikacji i przechowywane w tokenie programowym, takim jak PKCS#12.

[2] *Online Certificate Status Protocol*

2.2 Procedury walidacji tożsamości

W przypadku podsystemów wewnętrznych (*CCK MF Wewnętrzne* i *CCK MF Infrastruktura i Aplikacje*), weryfikacja tożsamości jest realizowana w oparciu o wewnętrzne procedury Ministerstwa Finansów. W przypadku podsystemów zewnętrznych (*CCK MF Zewnętrzne* i *CCK KSeF*), tożsamość subskrybenta jest walidowana podczas zakładania odpowiedniego konta w PUESC[3] lub – w przypadku KSeF[4] – w celu złożenia wniosku o wydanie certyfikatu użytkownik musi uwierzytelnić się i zautoryzować w KSeF, po czym składa wniosek za pośrednictwem tego systemu.

System PUESC

Potwierdzenie tożsamości w ramach uzyskiwania konta PUESC z rozszerzonym zakresem uprawnień jest możliwe na podstawie:

- podpisania wniosku podpisem kwalifikowanym,
- podpisania wniosku podpisem zaufanym,
- osobistego stawiennictwa i wylegitymowania się dokumentem tożsamości (dowód osobisty, paszport, karta stałego pobytu) w:
  - urzędzie celno-skarbowym;
  - delegaturze urzędu celno-skarbowego lub
  - oddziale celnym.

W przypadku obywateli kraju trzeciego (spoza UE), można potwierdzić autentyczność danych rejestracyjnych:

- w konsulacie,
- w ambasadzie,
- u notariusza w kraju zamieszkania.

Zasady potwierdzania tożsamości opisane są na stronie
https://puesc.gov.pl/web/guest/uslugi/sposoby-potwierdzania-tozsamosci-osoby

System KSeF

Potwierdzenie tożsamości w ramach KSeF jest możliwe na podstawie:

- podpisania wniosku podpisem kwalifikowanym (certyfikat kwalifikowany musi zawierać nr PESEL),
- opieczętowania wniosku pieczęcią kwalifikowaną (certyfikat kwalifikowany musi zawierać nr NIP),
- podpisania wniosku podpisem zaufanym (weryfikowanym Profilem Zaufanym ePUAP)[5]
- pieczęci elektronicznej weryfikowanej EE certyfikatem AP Peppol[6]
- uwierzytelnienia za pośrednictwem Krajowego Węzła Identyfikacji Elektronicznej[7] o poziomie bezpieczeństwa „średni" lub „wysoki".

Uwierzytelnienie może być również dokonane na podstawie poprzedniego certyfikatu (na podstawie ważnego podpisu/pieczęci osoby ubiegającej się o certyfikat). W takim przypadku nowy certyfikat będzie zawierał te same dane identyfikujące Subskrybenta, co dane w poprzednim certyfikacie.

2.3 Użycie certyfikatów

W ramach niniejszej polityki certyfikacji dla subskrybentów generowane są następujące certyfikaty:

- podsystem *CCK MF Zewnętrzne* – certyfikaty celne, do podpisywania dokumentów przesyłanych do KAS,

[3] Platforma Usług Elektronicznych Skarbowo-Celnych

[4] Krajowy System e-Faktur

[5] https://www.biznes.gov.pl/pl/portal/0074

[6] https://efaktura.gov.pl/openpeppol/

[7] https://www.gov.pl/web/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej

- podsystem *CCK MF Wewnętrzne* - certyfikaty celne dla pracowników/funkcjonariuszy KAS i MF (1) do podpisywania i (2) do szyfrowania,
- podsystem *CCK MF Infrastruktura i aplikacje* – certyfikaty dla usług i urządzeń, certyfikaty aplikacyjne, certyfikaty do zabezpieczania komunikacji i danych, również w zakresie wymiany z podmiotami zewnętrznymi, certyfikaty pieczęci elektronicznych, znakowania czasem, OCSP,
- podsystem *CCK KSeF* – certyfikaty na potrzeby uwierzytelniania oraz potwierdzania faktur w trybach offline KSeF.

W związku z powyższym CCK MF wydaje certyfikaty o różnorodnym typie zastosowań, **przy czym ich wykorzystanie ogranicza się do potrzeb wewnętrznych jednostek podległych ministrowi właściwemu do spraw finansów**, jak również do komunikacji między obywatelami a tymi jednostkami w sprawach dotyczących załatwiania spraw prowadzonych w ramach usług realizowanych drogą elektroniczną. W szczególności certyfikaty CCK MF mają zastosowanie do uwierzytelniania dokumentów za pomocą zaawansowanego podpisu elektronicznego weryfikowanego za pomocą certyfikatu celnego, o którym mowa w art. 10b ustawy z dnia 19 marca 2004 r. „Prawo celne" oraz w § 4 pkt 3 „Rozporządzenia Ministra Rozwoju i Finansów z dnia 19 września 2017 r. w sprawie sposobu przesyłania deklaracji i podań oraz rodzajów podpisu elektronicznego, którymi powinny być opatrzone" oraz certyfikaty CCK MF służą do uwierzytelniania użytkowników i opatrywania kodem weryfikującym faktur w ramach KSeF.

3 Zakres gwarancji

CCK MF nie udziela żadnych domyślnie udzielanych gwarancji, poza mogącymi wynikać z obowiązujących przepisów prawa powszechnego. CCK MF nie wypłaca odszkodowań za szkody ani nie odpowiada za utracone korzyści subskrybentów.

CCK MF zachowuje następujące informacje przez co najmniej 20 lat po tym, jak jakikolwiek certyfikat oparty na tych dokumentach przestanie być ważny:

- dokumentację wytworzoną przy okazji akceptacji certyfikatu (tj. zgłoszenia konieczności korekty),
- wszystkie wydane certyfikaty,
- wszystkie wydane listy CRL[8].

4 Obowiązki subskrybentów

Subskrybent zobowiązany jest do podania prawdziwych danych podczas rejestracji. Wymaga się, aby subskrybent, na rzecz którego wystawiono certyfikat, zweryfikował prawidłowość danych zawartych w certyfikacie, bezpośrednio po jego otrzymaniu. W przypadku stwierdzenia nieprawidłowości, subskrybent powinien niezwłocznie poinformować o tym wydawcę certyfikatu i wystąpić z wnioskiem o wydanie nowego, dokonując uprzednio korekty wadliwych danych.

Subskrybent jest zobowiązany do należytej ochrony klucza prywatnego przed ujawnieniem lub wykorzystaniem przez osoby nieupoważnione. Klucz prywatny do podpisu elektronicznego powinien pozostać w wyłącznej gestii subskrybenta – osoby fizycznej, której dane są umieszczane w certyfikacie. Niedopuszczalne jest, aby klucz był używany przez inną osobę. Klucz prywatny do pieczęci elektronicznej powinien pozostać w wyłącznej gestii osoby lub osób upoważnionych przez daną osobę/organizację.

W przypadku uzasadnionego podejrzenia dostępu do klucza prywatnego przez osobę nieuprawnioną, utraty lub ujawnienia klucza prywatnego lub okoliczności, w których zachodzi ryzyko nieuprawnionego użycia klucza, subskrybent jest zobowiązany do niezwłocznego unieważnienia certyfikatu.

Certyfikaty CCK MF nie mogą być wykorzystywane przez osoby bądź podmioty zewnętrzne w stosunku do MF i jednostek podległych, w celu innym niż przekazywanie danych do systemów MF lub weryfikacja

[8] *Certificate Revocation List*

komunikatów przekazywanych z tych systemów. W szczególności certyfikaty emitowane przez *CCK MF Zewnętrzne*, *CCK MF Wewnętrzne*, *CCK MF Infrastruktura i Aplikacje* oraz *CCK KSeF* nie mogą służyć do potwierdzania tożsamości nadawcy w życiu prywatnym, czy w sprawach kierowanych do innych podmiotów bądź urzędów administracji publicznej, z wyjątkiem usług świadczonych za pośrednictwem platform elektronicznych Ministerstwa Finansów lub Krajowej Administracji Skarbowej oraz wewnętrznej wymiany informacji w jednostkach podległych ministrowi właściwemu do spraw finansów.

Polityka certyfikacji CCK MF nie nakłada obowiązku przechowywania kluczy abonenta w specjalnych urządzeniach, takich jak karty elektroniczne.

5 Obowiązki stron ufających w zakresie sprawdzania statusu certyfikatu

Jedynym sposobem potwierdzenia ważności certyfikatu subskrybenta pod kątem ewentualnego unieważnienia lub zawieszenia jest sprawdzenie statusu certyfikatu na odpowiedniej liście CRL lub skorzystanie z usługi OCSP, jednak usługa OCSP nie jest dostępna w każdym podsystemie certyfikacji.

Fakt, że nowa lista CRL nie została opublikowana w określonym czasie, nie może być podstawą do stwierdzenia, że certyfikaty nie zostały unieważnione.

Aby zbadać status unieważnienia certyfikatu, należy:

- pobrać token OCSP dla tego certyfikatu i sprawdzić status certyfikatu zapisany w tym tokenie lub
- pobrać listę CRL wystawioną po czasie, w którym badamy ważność certyfikatu i sprawdzić status certyfikatu na liście CRL.

Weryfikacja poprawności podpisów na certyfikatach, tokenach OCSP i listach CRL musi zostać przeprowadzona na podstawie ścieżki certyfikacji rozpoczynającej się od klucza publicznego Root (tzw. „kotwicy zaufania").

Należy zauważyć, że w podsystemie *CCK KSeF* lista CRL obejmuje krytyczne rozszerzenie issuingDistributionPoint, które umożliwia segmentację listy CRL na mniejsze części. Zgodnie z rozdziałem 5.2.5 dokumentu RFC 5280 (X.509) składnia i semantyka pola distributionPoint w tym rozszerzeniu są takie same jak pola distributionPoint w rozszerzeniu CRLDistributionPoints w certyfikatach. Jeśli pole distributionPoint jest obecne w rozszerzeniu issuingDistributionPoint, MUSI zawierać co najmniej jedną z nazw z odpowiadającego pola distributionPoint rozszerzenia cRLDistributionPoints każdego certyfikatu, który znajduje się w zakresie tej listy CRL (to samo kodowanie jest używane w polach distributionPoint certyfikatu i listy CRL).

6 Odpowiedzialność i ograniczenia

CCK MF jest zobligowane do:

- właściwego zabezpieczania swych kluczy prywatnych przed uszkodzeniem lub ujawnieniem,
- zapewnienia kontroli dostępu do sprzętu i oprogramowania używanego w CCK MF,
- terminowej realizacji żądań zawieszenia / unieważnienia certyfikatów,
- publikowania i utrzymywania aktualnych list CRL i tokenów OCSP (usługa OCSP nie jest implementowana we wszystkich podsystemach).

CCK MF nie ponosi odpowiedzialności za skutki niezgodnego z niniejszą polityką użycia certyfikatu wydanego subskrybentowi.

CCK MF, w ramach świadczenia usług zaufania, nie ponosi odpowiedzialności za poprawność działania oprogramowania wykorzystywanego przez subskrybenta/stronę ufającą oraz za poprawność

i adekwatność środków bezpieczeństwa technicznego i organizacyjnego stosowanych przez subskrybenta/stronę ufającą.

W żadnym razie CCK MF nie będzie odpowiadać za jakiekolwiek szkody subskrybentów i stron ufających (bądź innych stron) wynikłe, bądź w jakikolwiek sposób związane z nadużyciem lub wykorzystaniem certyfikatu wydanego przez CCK MF, który został:

- unieważniony lub wygasł,
- użyty w niedozwolonym celu,
- zmanipulowany (jego integralność nie została zweryfikowana pozytywnie),
- złamany (komplementarny klucz prywatny uległ kompromitacji),
- pominięty.

7 Obowiązujące umowy, Polityka certyfikacji

Niniejsze streszczenie dotyczy polityki certyfikacji, której dane identyfikacyjne podano w poniższej tabeli:

Nazwa polityki	Polityka certyfikacji Centrum Certyfikacji Ministerstwa Finansów
Kwalifikator polityki	brak
OID (ang. *Object Identifier*)	0.4.0.2042.1.3 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) lcp (3)
Wersja	2.3
Data zatwierdzenia	11.05.2026
Ważność	do odwołania

Pełny tekst dokumentu polityki certyfikacji dostępny jest na stronie internetowej:

https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf
lub
https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/

8 Ochrona danych osobowych

CCK MF przetwarza dane osobowe subskrybentów stosując obowiązujące przepisy w zakresie ich ochrony oraz wymagania określone w Polityce Ochrony Danych Osobowych obowiązującej w Resorcie Finansów.

9 Polityka zwrotów

Jeśli subskrybent nie jest zadowolony z usług, może poprosić o unieważnienie certyfikatu. CCK MF nie pobiera żadnych opłat za świadczone usługi, dlatego nie ma zwrotów opłat za wydany certyfikat.

10 Obowiązujące prawo, skargi i rozwiązywanie sporów

W zakresie stosowania niniejszej polityki certyfikacji prawem obowiązującym jest prawo polskie. W sprawach interpretacji jakichkolwiek postanowień zastosowanie mają przepisy prawa polskiego. Ewentualne spory, których rozwiązanie nie będzie możliwe na drodze polubownych rokowań, rozstrzygane będą przez sądy polskie.

11 Licencje, środki polepszające zaufanie i audyt

CCK MF podlega regularnym audytom wewnętrznym, prowadzonym przez osoby niezajmujące się bieżącą obsługą CCK MF, jak również audytom zewnętrznym.

Audyty bezpieczeństwa są prowadzone z zachowaniem obiektywności i bezstronności procesu audytu, w szczególności niezbędne jest zapewnienie, aby osoby realizujące audyt bezpieczeństwa nie były odpowiedzialne za przegląd tej części systemu, w której realizacji biorą udział w ramach obowiązków służbowych.

Osoby przeprowadzające audyt bezpieczeństwa posiadają odpowiednie kwalifikacje, doświadczenie oraz znajomość metodyki prowadzenia audytu bezpieczeństwa.

Zadania związane z prowadzeniem audytu bezpieczeństwa mogą zostać powierzone podmiotowi zewnętrznemu zapewniającemu:

- realizację zgodnie ze standardami audytowania systemów zarządzania bezpieczeństwem informacji określonymi w polskich i międzynarodowych normach, w tym ISO 19011,
- wykwalifikowanych audytorów, w tym audytora wiodącego, posiadających certyfikaty potwierdzające wiedzę w zakresie audytowania na zgodność z normą ISO 27001,
- odpowiednie doświadczenie potwierdzone referencjami.

Zewnętrzny audyt odbywa się nie rzadziej niż raz na 2 lata.

Wewnętrzna dokumentacja Ministerstwa Finansów zawiera dokument określający procedury audytu.

CCK MF znajduje się w rejestrze prowadzonym na podstawie i w zakresie rzeczowym określonym przepisem art. 6 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (tekst jednolity Dz.U. z 2024 r. poz. 1725). Minister właściwy do spraw informatyzacji nie nadzoruje takiego podmiotu ex ante, a działania może podejmować jedynie w przypadku zgłoszenia nieprawidłowości zgodnie z art. 17 ust. 3 pkt b rozporządzenia eIDAS[9].

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE