

**UKNF**

URZĄD  
KOMISJI  
NADZORU  
FINANSOWEGO

# Polityka Certyfikacji Centrum Certyfikacji Portalu KNF

Wersja 1.5

## Rejestr zmian w dokumencie

Data [RRRR-MM-DD]	Autor	Wersja	Opis zmian
2014-10-13	PWPW	1.0	Utworzenie dokumentu
2014-11-03	PWPW	1.1	Poprawki dokumentu uwzględniające uwagi UKNF do zgłoszenia odbioru z dnia 21.10.2014
2014-11-04	PWPW	1.2	Poprawki dokumentu uwzględniające uwagi UKNF do zgłoszenia odbioru z dnia 21.10.2014
2015-05-21	PWPW	1.3	Przegląd i aktualizacja dokumentu po instalacji produkcyjnej
2015-06-18	PWPW	1.4	Aktualizacja publikatora ustawy o ochronie danych osobowych
2015-07-24	Dariusz Górka	1.4	Aktualizacja atrybutów certyfikatów. Dodanie rozszerzenia *.crl w linkach do listy uknfportalsubca.crl
2022-02-01	Przemysław Baiński, Piotr Łodziński	1.5	Weryfikacja aktualności Polityki Certyfikacji

1	Wstęp .....	7
1.1	Nazwa dokumentu i jego identyfikacja.....	8
1.2	Strony Polityki Certyfikacji oraz zakres jej stosowania .....	8
1.2.1	Urząd certyfikacji .....	9
1.2.2	Urząd rejestracji.....	10
1.2.3	Subskrybenci.....	11
1.2.4	Podmioty ufające .....	11
1.2.5	Inni uczestnicy .....	12
1.3	Zakres stosowania certyfikatów .....	12
1.3.1	Dozwolone sposoby użycia .....	12
1.3.2	Zabronione sposoby użycia .....	12
1.4	Administrowanie Polityką Certyfikacji.....	13
1.4.1	Podmiot zarządzający dokumentacją.....	13
1.4.2	Osoba kontaktowa .....	13
1.4.3	Osoba odpowiedzialna za dostosowanie CPS do Polityki Certyfikacji.....	13
1.5	Definicje i skróty.....	13
2	Publikacja i odpowiedzialność repozytorium .....	14
2.1	Repozytorium.....	14
2.2	Publikacja informacji o certyfikacji .....	14
2.3	Czas lub częstotliwość publikacji .....	14
2.4	Dostęp do repozytorium .....	15
3	Identyfikacja i uwierzytelnianie.....	15
3.1	Nazewnictwo.....	15
3.1.1	Typy nazw .....	15
3.1.2	Konieczność używania nazw rozpoznawalnych.....	15
3.1.3	Anonimowość lub pseudonimy subskrybentów .....	15
3.1.4	Zasady interpretacji różnych form nazw .....	15
3.1.5	Unikatowość nazw .....	15
3.1.6	Rozpoznawanie, uwierzytelnianie oraz rola znaków handlowych.....	16
3.2	Wstępne potwierdzenie tożsamości .....	16
3.2.1	Uwierzytelnianie tożsamości osób fizycznych.....	16
3.2.2	Weryfikacja i potwierdzenie uprawnień.....	16
3.3	Identyfikacja i uwierzytelnianie dla wniosków o aktualizację kluczy.....	16
3.4	Identyfikacja i uwierzytelnianie dla wniosków o unieważnienie .....	16
4	Wymagania operacyjne dotyczące cyklu życia certyfikatów .....	17
4.1	Składanie wniosków o certyfikaty .....	17

4.1.1	Kto może wnioskować o certyfikat .....	17
4.1.2	Proces zgłaszania wniosków o certyfikat .....	17
4.2	Przetwarzanie wniosków o certyfikat .....	17
4.2.1	Identyfikacja i uwierzytelnianie wnioskodawcy .....	17
4.2.2	Zatwierdzenie lub odmowa wniosku o certyfikat.....	17
4.2.3	Czas na przetworzenie wniosku o certyfikat .....	17
4.3	Wydanie certyfikatu .....	18
4.3.1	Czynności CA podczas wydawania certyfikatu .....	18
4.3.2	Powiadomienie subskrybenta o wydaniu certyfikatu przez CA.....	19
4.4	Akceptacja certyfikatu .....	20
4.4.1	Czynności związane z akceptacją certyfikatu.....	20
4.4.2	Publikacja certyfikatu przez CA.....	20
4.4.3	Powiadomienie innych podmiotów o wydaniu certyfikatu przez CA .....	20
4.5	Zakres używania pary kluczy i certyfikatów .....	20
4.5.1	Zakres używania klucza prywatnego subskrybenta i certyfikatu .....	20
4.5.2	Zakres używania klucza publicznego przez podmioty ufające.....	21
4.6	Odnowienie certyfikatu .....	21
4.7	Aktualizacja klucza certyfikatu.....	22
4.8	Modyfikacja certyfikatu .....	22
4.8.1	Okoliczności modyfikacji certyfikatu.....	22
4.8.2	Kto może wnioskować o modyfikację certyfikatu .....	22
4.8.3	Przetwarzanie wniosków o modyfikację certyfikatów .....	22
4.8.4	Powiadomienie subskrybenta o wydaniu zmodyfikowanego certyfikatu .....	22
4.8.5	Czynności związane z akceptacją zmodyfikowanego certyfikatu.....	22
4.8.6	Publikacja zmodyfikowanego certyfikatu przez CA .....	22
4.8.7	Powiadomienie innych podmiotów o wydaniu certyfikatu przez CA .....	23
4.9	Unieważnienie i zawieszenie certyfikatu .....	23
4.9.1	Okoliczności unieważnienia certyfikatu.....	23
4.9.2	Kto może wnioskować o unieważnienie certyfikatu .....	23
4.9.3	Procedura dla wniosku o unieważnienie certyfikatu .....	23
4.9.4	Czas odroczenia prośby o unieważnienie certyfikatu.....	23
4.9.5	Czas, w którym CA musi przetworzyć wniosek o unieważnienie.....	24
4.9.6	Obowiązek sprawdzania unieważnionych certyfikatów przez podmioty ufające	24
4.9.7	Częstotliwość publikowania list CRL (jeśli konieczne).....	24

4.9.8	Maksymalne opóźnienie publikacji list CRL (jeśli konieczne).....	24
4.9.9	Dostępność sprawdzenia bieżącego statusu unieważnienia .....	24
4.9.10	Wymagania dotyczące bieżącego sprawdzania unieważnienia.....	24
4.9.11	Inne dostępne formy zgłaszania stanu unieważnienia.....	24
4.9.12	Wymogi specjalne odnośnie kompromitacji klucza.....	24
4.9.13	Okoliczności zawieszenia certyfikatu.....	25
4.9.14	Kto może wnioskować o zawieszenie .....	25
4.9.15	Procedura dla wniosków o zawieszenie .....	25
4.9.16	Ograniczenia, co do okresu zawieszenia .....	25
4.10	Usługi związane ze statusem certyfikatu .....	25
4.10.1	Charakterystyka funkcjonalności.....	25
4.10.2	Dostępność usług .....	25
4.10.3	Dodatkowe funkcje.....	25
4.11	Czas wygaśnięcia .....	26
4.12	Deponowanie i odtworzenie kluczy .....	26
5	Zabezpieczenia fizyczne i organizacyjne.....	26
6	Zabezpieczenia techniczne.....	26
7	Profile certyfikatów, list CRL i OCSP.....	26
8	Audyt i inne sposoby oceny.....	27
9	Pozostałe zagadnienia i kwestie prawne.....	27
9.1	Opłaty.....	27
9.2	Odpowiedzialność finansowa.....	27
9.3	Poufność informacji .....	27
9.3.1	Zakres informacji poufnych.....	27
9.3.2	Informacje będące poza zakresem poufności .....	28
9.3.3	Odpowiedzialność za ochronę informacji poufnych .....	28
9.4	Ochrona danych osobowych .....	28
9.5	Prawo do własności intelektualnej.....	28
9.6	Rękojmie i gwarancje.....	29
9.7	Zastrzeżenia gwarancji.....	29
9.8	Ograniczenia odpowiedzialności .....	29
9.9	Odszkodowania.....	29
9.10	Okres obowiązywania i wygaśnięcie .....	29
9.10.1	Okres obowiązywania.....	29
9.10.2	Wygaśnięcie.....	30
9.10.3	Efekty wygaśnięcia.....	30

9.11	Powiadomienia indywidualne oraz kontakt z uczestnikami .....	30
9.12	Poprawki .....	30
9.13	Ustalenia, co do rozstrzygania sporów.....	30
9.15	Zgodność ze stosownymi przepisami prawa.....	31
9.16	Pozostałe ustalenia .....	31
9.16.1	Całość porozumienia .....	31
9.16.2	Cesja .....	31
9.16.3	Rozdzielność postanowień umowy.....	31
9.16.4	Egzekwowanie.....	31
9.16.5	Siła wyższa .....	31
9.17	Pozostałe ustalenia .....	31

## 1 Wstęp

**Polityka Certyfikacji Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** (nazywana dalej Polityką Certyfikacji lub w skrócie PC) określa wymagania techniczne i organizacyjne dla tworzenia i stosowania certyfikatów klucza publicznego wydawanych przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**. **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** działa w ramach systemu Infrastruktury Klucza Publicznego (PKI) **Urzędu Komisji Nadzoru Finansowego**.

Polityka Certyfikacji musi być rozpatrywana łącznie z **Kodeksem Postępowania Certyfikacyjnego Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** (nazywany dalej Kodeksem Postępowania Certyfikacyjnego).

Polityka Certyfikacji reguluje podstawowe prawa i obowiązki stron: **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** i subskrybentów (użytkowników tego systemu) oraz stron ufających. Kodeks Postępowania Certyfikacyjnego określa, w jaki sposób zapewnia się gwarantowany przez Politykę Certyfikacji poziom zaufania.

Zapoznanie się z dokumentami Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego jest istotne w przypadku zawierania umów certyfikacyjnych z subskrybentami i stronami ufającymi.

Struktura Polityki Certyfikacji oparta jest na zaleceniach RFC 3647.

W niniejszym dokumencie zostały opisane zasady działania **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

Do zasad obowiązujących w dokumencie Polityki Certyfikacji powinny dostosować się podmioty korzystające z usług **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

## 1.1 Nazwa dokumentu i jego identyfikacja

Niniejszy dokument przypisaną ma nazwę własną: **Polityka Certyfikacji Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**. Cytowanie tego dokumentu powinno odnosić się do przedstawionych w dokumencie form.

Dokument Polityki Certyfikacji dostępny jest w postaci:

1. Elektronicznej, w repozytorium pod adresem <https://bip.knf.gov.pl/>.
2. Elektronicznej, jeżeli zainteresowany wyśle żądanie na adres email: [knf@knf.gov.pl](mailto:knf@knf.gov.pl).
3. Papierowej, dostępnej w siedzibie **Urzędu Komisji Nadzoru Finansowego**.

Poniżej przedstawione zostało podsumowanie informacji o Polityce Certyfikacji.

**Tabela 1 Informacje o Polityce Certyfikacji**

Parametr	Wartość
Nazwa	<b>Polityka Certyfikacji Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego</b>
Instytucja realizująca	<b>Urząd Komisji Nadzoru Finansowego</b>
Zastrzeżenie	Brak
Wersja	1.5
Identyfikator polityki OID	Nie dotyczy
Data wydania	
Data ważności	Do odwołania
Status	Obowiązujący
Kodeks Postępowania Certyfikacyjnego związany z Polityką Certyfikacji	<b>Kodeks Postępowania Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego.</b>

## 1.2 Strony Polityki Certyfikacji oraz zakres jej stosowania

**Polityka Certyfikacji Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** obejmuje swoim zakresem:

1. **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** zarządzane przez **Urząd Komisji Nadzoru Finansowego**.
2. **Urząd certyfikacji – UKNF Portal CA.**
3. **Urząd rejestracji.**
4. **Repozytorium.**
5. **Subskrybentów.**
6. **Podmioty ufające.**
7. **Innych uczestników.**

**Centrum Certyfikacji Portalu Urzędu Komisji Nadzoru Finansowego** dostarcza usługi certyfikacyjne na potrzeby użytkowników **Portalu Urzędu Komisji Nadzoru Finansowego**.

Usługi te obejmują:

1. **Wydawanie certyfikatów**
2. **Unieważnianie certyfikatów**



### 3. Udostępnianie informacji o statusie certyfikatu

Powyższe usługi świadczone są osobom fizycznym, które w pełni akceptują zasady zawarte w niniejszym dokumencie.

#### 1.2.1 Urząd certyfikacji

W skład **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** wchodzi urząd certyfikacji.

**Tabela 2 Nazwy serwerów i CA.**

Nazwa CA	Opis
UKNF Portal CA	Urząd Certyfikacji dla użytkowników Portalu KNF

Urząd **UKNF Portal CA** pracuje w strukturze urzędów certyfikacji **Urzędu Komisji Nadzoru Finansowego** i wydaje certyfikaty dla uprawnionych subskrybentów - użytkowników **Portalu Komisji Nadzoru Finansowego**.

##### 1.2.1.1 Obowiązki urzędu certyfikacji

**Centrum Certyfikacji Portalu Urzędu Komisji Nadzoru Finansowego** zobowiązuje się każdorazowo do podjęcia odpowiednich kroków mających na celu weryfikację informacji związanych z tożsamością subskrybenta występującego o certyfikat, weryfikację informacji związanych z wydawanym certyfikatem, tj. aktualność, zawartość oraz wykonanie pozostałych czynności związanych z procesem certyfikacji. Sposób weryfikacji tożsamości subskrybenta zależy od typu subskrybenta.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** gwarantuje, że w przypadku zaistnienia podejrzenia, że zawartość certyfikatu nie jest aktualna lub klucz prywatny został skompromitowany, odpowiedni certyfikat zostanie unieważniony.

Informacje o czynnościach, takich jak wydanie unieważnienia certyfikatu, zawsze są udostępniane innym, zainteresowanym wystąpieniem takich zdarzeń, subskrybentom.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** zobowiązuje się do:

1. Świadczenia usług certyfikacyjnych polegających na wydawaniu certyfikatów klucza publicznego na podstawie otrzymanych wniosków.
2. Zapewnienia ochrony danych osobowych subskrybenta na podstawie przepisów prawa powszechnie obowiązującego w tym w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
3. Respektowania praw subskrybentów i podmiotów ufających wynikających z przepisów prawa, regulacji **Urzędu Komisji Nadzoru Finansowego** i obowiązujących oświadczeń i porozumień.
4. Zapewnienia odpowiedniej długości certyfikowanych kluczy publicznych.
5. Zapewnienia odpowiedniej struktury certyfikowanych kluczy publicznych.
6. Zapewnienia unikalności nazw wyróżnionych (DN) stosowanych w certyfikatach, w obrębie domeny własnej.

7. Utrzymywania ogólnodostępnego repozytorium do publikowania certyfikatów, list unieważnionych certyfikatów i polityki certyfikacji.
8. Terminowego publikowania informacji niezbędnych do prawidłowego funkcjonowania usług certyfikacyjnych np. informacje o unieważnianiu certyfikatów.
9. Stosowania wiarygodnych algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych.
10. Utrzymywania listy unieważnionych certyfikatów oraz obsługi zleceń unieważniania certyfikatów
11. Zarchiwizowania kluczy, w przypadku, gdy klucze te stosowane są do deszyfrowania informacji.

#### 1.2.1.2 Odpowiedzialność urzędu certyfikacji

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** ponosi odpowiedzialność za:

1. Skutki działań urzędu certyfikacji **UKNF Portal CA**.
2. Informacje i certyfikaty publikowane w repozytorium.

**UWAGA: Przedstawione zasady dotyczące odpowiedzialności stron nie mogą zastępować odpowiedzialności wynikającej z odrębnych przepisów prawa.**

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie odpowiada za:

1. Zdarzenia losowe niezależne od sposobu funkcjonowania **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** tj. pożaru, powodzi oraz innych klęsk żywiołowych.
2. Szkody spowodowane przez umyślne lub nieumyślne działania człowieka, np. akty terroru.
3. Działania stron trzecich oraz subskrybentów.
4. Szkody wynikłe z niewłaściwego stosowania kluczy lub certyfikatów.

### 1.2.2 Urząd rejestracji

#### 1.2.2.1 Obowiązki urzędu rejestracji

Urząd rejestracji, który prowadzi działalność w ramach **Centrum Certyfikacji Portalu Urzędu Komisji Nadzoru Finansowego**, zobowiązany jest do:

1. Podporządkowania się wymaganiom i zaleceniom **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, poza przypadkami określonymi w procedurach zarządzania urzędem rejestracji.
2. Do dochowania należytej staranności w zakresie weryfikowania tożsamości subskrybentów wymaganej podczas wydawania i unieważniania certyfikatów zgodnie z zasadami opisanymi w niniejszej Polityce Certyfikacji oraz procedurami wewnętrznymi i obowiązującymi przepisami prawa.
3. Przesyłania do Urzędu Certyfikacji potwierdzonych informacji o subskrybencie.
4. Poddawania się planowym audytom prowadzonym lub zlecanym przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

### **1.2.2.2 Odpowiedzialność urzędu rejestracji**

Urząd rejestracji ponosi odpowiedzialność w przypadkach, gdy szkody poniesione przez subskrybentów i strony ufające są wynikiem naruszenia przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** gwarancji i zobowiązań przedstawionych w pkt. 1-2 poprzedniego paragrafu, chyba, że niewywiązanie się z tych obowiązków i gwarancji jest następstwem okoliczności, za które **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie ponosi odpowiedzialności i którym nie mogło zapobiec mimo dołożenia należytej staranności.

### **1.2.3 Subskrybenci**

Subskrybentami, są użytkownicy **Portalu Komisji Nadzoru Finansowego**.

#### **1.2.3.1 Obowiązki subskrybentów**

Subskrybenci **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** zobowiązani są do:

1. Przestrzegania zasad wykorzystania certyfikatów określonych przez **Urząd Komisji Nadzoru Finansowego**.
2. Przestrzegania zasad i ograniczeń zawartych w niniejszym dokumencie odnośnie sposobu używania certyfikatów i innych działań mieszczących się w zakresie oferowanych przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** usług certyfikacyjnych.
3. Informowania **Urzędu Komisji Nadzoru Finansowego** o zmianach w danych osobowych subskrybenta np. zmiana nazwiska.
4. Zaznajomienia się z podstawowymi pojęciami dotyczącymi infrastruktury klucza publicznego (PKI).
5. Zaznajomienia się z treścią certyfikatu klucza publicznego i zwrócenie uwagi na status certyfikatu, czy nie został unieważniony, przeterminowany.
6. Niezwłocznego poinformowania **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** – wystawcy certyfikatu, o podejrzeniu naruszenia ochrony swojego klucza prywatnego

### **1.2.4 Podmioty ufające**

Podmiot ufający definiowany jest, jako dowolny podmiot, korzystający z usług **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, którego decyzje zależą od statusu relacji pomiędzy tożsamością subskrybenta a jego kluczem publicznym, potwierdzonym przez urząd certyfikacji **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**. Uogólniając, podmiot ufający posługuje się certyfikatem innego podmiotu w celu zweryfikowania jego podpisu cyfrowego lub dochowania poufności przesyłanych danych.

#### **1.2.4.1 Obowiązki podmiotów ufających**

Podmiot ufający zobowiązany jest do:

1. Przestrzegania zasad i ograniczeń zawartych w niniejszym dokumencie odnośnie sposobu używania certyfikatów i innych działań mieszczących się w zakresie oferowanych przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**

usług certyfikacyjnych.

2. Zweryfikowania statusu używanego certyfikatu w oparciu o repozytorium unieważnionych certyfikatów lub serwer OCSP i zasady zawarte w niniejszym dokumencie.
3. Podjęcia odpowiednich kroków w przypadku stwierdzenia nieprawidłowości w certyfikacie. Certyfikat taki nie powinien zostać zaakceptowany i o nieprawidłowym Certyfikacie powinno zostać powiadomione **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

### 1.2.5 Inni uczestnicy

Nie dotyczy.

### 1.3 Zakres stosowania certyfikatów

Zakres stosowania certyfikatów obejmuje zasady związane z charakterem certyfikatów oraz zasady określające rekomendowane lub zabronione sposoby użycia.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** wydaje certyfikaty do uwierzytelniania użytkowników do **Portalu Komisji Nadzoru Finansowego**, oraz certyfikaty niezbędne do działania infrastruktury **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

Typy wydawanych certyfikatów zostały opisane poniżej:

**Tabela 3 Typy certyfikatów**

Typ certyfikatu	Przeznaczenie certyfikatu
Certyfikaty użytkownika <b>Portalu Komisji Nadzoru Finansowego</b>	Certyfikaty do uwierzytelniania użytkowników do <b>Portalu Komisji Nadzoru Finansowego</b>
Certyfikaty „infrastrukturalne”	Służą do wewnętrznych zastosowań <b>Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego</b>

#### 1.3.1 Dozwolone sposoby użycia

Certyfikaty wystawione przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** mogą być stosowane do:

1. Uwierzytelniania do **Portalu Komisji Nadzoru Finansowego**.
2. Ochrony dostępu do systemów **Portalu Komisji Nadzoru Finansowego**.

#### 1.3.2 Zabronione sposoby użycia

Zabronione jest wykorzystanie certyfikatów wystawionych przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** do innych celów niż opisane w rozdziale powyżej w tym dokumencie.

Zabronione jest wykorzystanie certyfikatów

1. Co do których podejrzewa się naruszenie wiarygodności.
2. Odwołanych i przeterminowanych.

## **1.4 Administrowanie Polityką Certyfikacji**

Poszczególne wersje Polityki Certyfikacji obowiązują do czasu opublikowania i zatwierdzenia nowej wersji. Uznaje się, że bieżąca dokumentacja Polityki Certyfikacji, która obowiązuje w danym momencie, przyznawany ma status: **AKTUALNA**.

Każda nowopowstała wersja polityki przekazywana jest do zatwierdzenia. Polityka Certyfikacji poddawana procedurze zatwierdzania ma status: **W ZATWIERDZANIU**. Zakończenie tej procedury powoduje, że nowa wersja polityki osiąga status **AKTUALNA**. Przedstawione zasady administrowania Polityką Certyfikacji obowiązują także w Kodeksie Postępowania Certyfikacyjnego.

Aktualne dokumenty Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego są dokumentami, do których subskrybenci muszą się zawsze stosować. Zasady zawarte w tych dokumentach są wiążące dla osób korzystających z usług certyfikacyjnych **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

### **1.4.1 Podmiot zarządzający dokumentacją**

**Urząd Komisji Nadzoru Finansowego**

**ul. Piękna 20**

**00-549 Warszawa**

**NIP: 7010902185**

tel. (48) 22 262-50-00

fax (48) 22 262-51-11

e-mail: knf@knf.gov.pl

### **1.4.2 Osoba kontaktowa**

Kierownik Zespołu Utrzymania Aplikacji

### **1.4.3 Osoba odpowiedzialna za dostosowanie CPS do Polityki Certyfikacji**

Kierownik Zespołu Utrzymania Aplikacji

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** ponosi odpowiedzialność za zgodność niniejszego dokumentu z następującymi regulacjami:

1. Przepisy polskiego prawa.
2. Dokument RFC 3647.
3. Wymagania organizacyjne oraz funkcjonalne **Urzędu Komisji Nadzoru Finansowego**.

## **1.5 Definicje i skróty**

- 1) Certyfikat – certyfikat elektroniczny służący do uwierzytelnienia.
- 2) Czas – czas wystawienia i unieważnienia certyfikatu, zgodnie z czasem uniwersalnym koordynowanym UTC(PL).
- 3) Lista CRL – lista unieważnionych certyfikatów dostawcy usług zaufania.
- 4) Organ nadzoru – minister właściwy do spraw informatyzacji.

- 5) Polityka świadczenia usług – nazwany zestaw reguł, w szczególności takich jak polityka certyfikacji, mający zastosowanie do określonego kręgu podmiotów lub zastosowań, o wspólnych dla tego kręgu wymaganiach bezpieczeństwa.
- 6) Repozytorium – strona internetowa <http://pki.knf.gov.pl/pki/uknfportalca2019.crl>, na której publikowane są w szczególności certyfikaty, listy unieważnionych certyfikatów.
- 7) Strona ufająca – to osoba fizyczna lub prawna, która polega na identyfikacji elektronicznej lub usłudze zaufania.
- 8) Subskrybent – kwalifikowany dostawca usług zaufania.
- 9) OCSP (Online Certificate Status Protocol) – usługa sprawdzenia statusu certyfikatu.
- 10) Portal KNF – system informatyczny używany w UKNF.

## 2 Publikacja i odpowiedzialność repozytorium

### 2.1 Repozytorium

Repozytorium jest zbiorem publicznie dostępnych informacji o certyfikatach wystawionych przez urząd certyfikacji. W repozytorium znajdują się

1. Certyfikaty poszczególnych Urzędów Certyfikacji.
2. Listy CRL poszczególnych Urzędów Certyfikacji.

Repozytorium **Centrum Certyfikacji Portalu Urzędu Komisji Nadzoru Finansowego** dostępne jest za pośrednictwem protokołu HTTP pod adresem: <http://pki.knf.gov.pl/pki/uknfportalca2019.crl>

### 2.2 Publikacja informacji o certyfikacji

Wszystkie informacje publikowane przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** dostępne są w repozytorium pod adresem: <http://pki.knf.gov.pl/pki/uknfportalca2019.crl>

### 2.3 Czas lub częstotliwość publikacji

Publikację w repozytorium **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** ogłasza się z następującą częstotliwością:

**Tabela 4 Częstotliwość publikowania w repozytorium**

<b>Publikowany materiał</b>	<b>Częstotliwość publikowania</b>
<b>Polityka Certyfikacji, Kodeks Postępowania Certyfikacyjnego</b>	Każdorazowo, gdy nastąpi ich uaktualnienie
<b>Certyfikaty urzędów certyfikacji funkcjonujących w ramach Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego</b>	Każdorazowo, gdy nastąpi wydanie nowych certyfikatów

<b>Certyfikaty subskrybentów</b>	Każdorazowo, gdy nastąpi wydanie nowych certyfikatów. Publikacja odbywa się w wewnętrznych repozytoriach <b>Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego</b>
<b>Listy certyfikatów unieważnionych</b>	Każdorazowo, gdy nastąpi wydanie nowych list. Dla urzędów podrzędnych, nie rzadziej, niż co 30 dni
<b>Informacje pomocnicze</b>	Każdorazowo, gdy nastąpi ich uaktualnienie

## 2.4 Dostęp do repozytorium

Wszystkie informacje publikowane przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** w repozytorium pod adresem: <http://pki.knf.gov.pl/pki/uknfportalca2019.crl> są dostępne publicznie.

## 3 Identyfikacja i uwierzytelnianie

Rozdział ten omawia zasady stosowane przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, podczas wydawania certyfikatów, przy weryfikacji tożsamości subskrybentów. Zasady te definiują środki, które podejmuje się w celu sprawdzenia dokładności i wiarygodności informacji podawanej przez subskrybentów.

### 3.1 Nazewnictwo

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** wydaje certyfikaty zgodne ze standardem X.509 v3, co oznacza, że stosowane są tylko te nazwy, które są nim zgodne.

#### 3.1.1 Typy nazw

Nazwy subskrybentów oraz nazwy wystawców certyfikatów umieszczane w certyfikatach są zgodne z nazwami wyróżnionymi DN.

#### 3.1.2 Konieczność używania nazw rozpoznawalnych

Nazwa wyróżniona DN musi być znacząca tzn. pozwalać na jednoznaczne określenie tożsamości jednostki w odpowiedniej sytuacji. Wymaganie to dotyczy zarówno subskrybentów, jak i urzędów certyfikacji.

#### 3.1.3 Anonimowość lub pseudonimy subskrybentów

Subskrybenci nie mogą pozostawać anonimowi.

#### 3.1.4 Zasady interpretacji różnych form nazw

Wiele języków obcych posiada zróżnicowane alfabety. Niektóre znaki nie znajdują się w standardowej tablicy znaków ASCII. Tam gdzie to konieczne, znaki takie jak: ą, ć, ę, ł, ń, ó, ś, ź, ż zastąpione zostały odpowiednio przez znaki: a, c, e, l, n, o, s, z, z.

#### 3.1.5 Unikatowość nazw

**Urząd Komisji Nadzoru Finansowego** gwarantuje, w ramach swojej domeny, unikalność przydzielonej subskrybentowi nazwy DN. Dzięki takiemu rozwiązaniu każdy subskrybent może zostać odpowiednio zidentyfikowany.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** rezerwuje sobie prawo podejmowania wszelkich decyzji dotyczących składni nazwy subskrybenta używanych w certyfikatach i przydzielania mu wynikłych z tego nazw.

### **3.1.6 Rozpoznawanie, uwierzytelnianie oraz rola znaków handlowych**

Nazwa **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** wykorzystywana jest przez **Urząd Komisji Nadzoru Finansowego** w certyfikatach i dokumentach wyłącznie w celach opisu i identyfikacji.

Logo i znaki towarowe używane w witrynach i dokumentach projektu wykorzystane są z poszanowaniem zasad prawa.

### **3.2 Wstępne potwierdzenie tożsamości**

Proces wstępnego potwierdzenia tożsamości rozpoczyna się w momencie, gdy subskrybent składa wniosek o dostęp do **Portalu Komisji Nadzoru Finansowego**.

#### **3.2.1 Uwierzytelnianie tożsamości osób fizycznych**

Uwierzytelnienie tożsamości osób fizycznych ma na celu wykazanie, że:

1. Dane podane we wniosku identyfikują istniejącą osobę fizyczną.
2. Osoba składająca wniosek jest rzeczywiście tą osobą fizyczną, której dane podane są we wniosku.
3. Osoba odbierająca certyfikaty i klucze jest osobą upoważnioną.

Uwierzytelnianie odbywa się na podstawie procedur organizacyjnych **Urzędu Komisji Nadzoru Finansowego**.

#### **3.2.2 Weryfikacja i potwierdzenie uprawnień**

Subskrybent wnoszący o dostęp do **Portalu Komisji Nadzoru Finansowego** i wnioskuje równocześnie o wydanie certyfikatu. Administratorzy Portalu wysyłają wniosek o certyfikat do **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**. Wniosek rozpatrywany jest zgodnie z procedurami organizacyjnymi **Portalu Komisji Nadzoru Finansowego**.

### **3.3 Identyfikacja i uwierzytelnianie dla wniosków o aktualizację kluczy**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie stosuje mechanizmu aktualizacji kluczy. Certyfikaty wydawane są na nowo z nowo wygenerowanymi kluczami.

### **3.4 Identyfikacja i uwierzytelnianie dla wniosków o unieważnienie**

Unieważnienie certyfikatu odbywa się na podstawie wniosku subskrybenta lub upoważnionych pracowników **Urzędu Komisji Nadzoru Finansowego**.

Wnioski o unieważnienie certyfikatów użytkowników:

1. Zewnętrznych składane są pisemnie na adres **Urzędu Komisji Nadzoru Finansowego**.
2. Wewnętrznych poprzez zgłoszenie ServiceDesk UKNF

Wnioski powinny umożliwiać jednoznaczną identyfikację tożsamości subskrybenta.

Identyfikacja tożsamości subskrybenta prowadzona jest na podstawie procedur organizacyjnych **Urzędu Komisji Nadzoru Finansowego**.



## 4 Wymagania operacyjne dotyczące cyklu życia certyfikatów

### 4.1 Składanie wniosków o certyfikaty

Wnioski o certyfikat może składać subskrybent lub osoba upoważniona działająca w jego imieniu. Certyfikat może zostać wydany tylko na podstawie złożonego wniosku. Wnioski przekazywane są do urzędu certyfikacji.

#### 4.1.1 Kto może wnioskować o certyfikat

Wniosek o certyfikat może złożyć administrator **Portalu Komisji Nadzoru Finansowego** w imieniu użytkownika portalu.

#### 4.1.2 Proces zgłaszania wniosków o certyfikat

Wnioski o certyfikat składane są pisemnie lub drogą elektroniczną poprzez przesłanie ich do **Urzędu Komisji Nadzoru Finansowego**.

Wniosek musi zawierać wszystkie niezbędne do identyfikacji i wystawienia certyfikatu dane subskrybenta. Proces składania wniosków określa Regulamin korzystania z Portalu Komisji Nadzoru Finansowego.

## 4.2 Przetwarzanie wniosków o certyfikat

### 4.2.1 Identyfikacja i uwierzytelnianie wnioskodawcy

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** dokona weryfikacji tożsamości subskrybenta na podstawie danych podawanych przez niego we wniosku o certyfikację. Proces weryfikacji tożsamości został określony w Regulaminie korzystania z Portalu Komisji Nadzoru Finansowego.

### 4.2.2 Zatwierdzenie lub odmowa wniosku o certyfikat

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** zatwierdzi wniosek o certyfikację wtedy i tylko wtedy, gdy zostaną spełnione następujące kryteria:

1. Wszystkie potrzebne informacje zostaną wypełnione we wniosku, dostarczone i zatwierdzone.
2. Proces identyfikacji subskrybenta zostanie zakończony z rezultatem pozytywnym.

Spełnienie powyższych warunków warunkuje wystawienie przez urząd certyfikatu.

Jeżeli wnioskodawca nie będzie spełniał powyższych warunków lub też z innego powodu uzna się, że nie spełnia ogólnie przyjętego kryterium certyfikacji, **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** ma prawo odmówić wydania certyfikatu.

### 4.2.3 Czas na przetworzenie wniosku o certyfikat

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** zatwierdzi wniosek bez opóźnień jak tylko:

1. Wszystkie potrzebne informacje zostaną wypełnione we wniosku, dostarczone i zatwierdzone.
2. Proces identyfikacji subskrybenta zostanie zakończony z rezultatem pozytywnym.

Przyjmuje się, że maksymalny czas na przetworzenie wniosku wynosi 7 dni.

W przypadku, gdy subskrybent wnoszący o certyfikację nie dostarczy potrzebnych danych do **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** w tym czasie, wniosek zostanie odrzucony.

### 4.3 Wydanie certyfikatu

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** weryfikuje wnioski z najwyższą dokładnością, sprawdza się m.in. dane osobowe subskrybenta. Pomyślna weryfikacja warunkuje wydanie certyfikatu. Subskrybent otrzymujący certyfikat ma zadanie sprawić, czy jego zawartość zgadza się z danymi, które zostały wprowadzone we wniosku. W przypadku jakichkolwiek nieprawidłowości lub wątpliwości należy się niezwłocznie zgłosić do osoby kontaktowej przedstawionej w niniejszym dokumencie.

#### 4.3.1 Czynności CA podczas wydawania certyfikatu

Urząd certyfikacji **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, po otrzymaniu odpowiedniego wniosku oraz zweryfikowaniu poprawności i zasadności wniosku subskrybenta, wydaje certyfikat. Wydawanie certyfikatów może odbywać się na następujące sposoby:

1. Standardowe wydanie certyfikatu dla pierwszego Administratora w podmiocie.
2. Uprozczone wydanie certyfikatu dla Administratora w podmiocie, który jest już zarejestrowany w Portalu.
3. Obsługa certyfikatów użytkowników merytorycznych w podmiocie przez Administratora podmiotu (dotyczy również innych administratorów w danym podmiocie).
4. Obsługa certyfikatów użytkowników merytorycznych lub technicznych podmiotów utworzonych w celu zapewnienia korespondencji z Powiernikami banków hipotecznych przez Administratora Portalu. Administrator Portalu pełni w tym przypadku funkcję i ma konto Administratora podmiotu .

**Tabela 5 Sposoby wydawania certyfikatów.**

Sposób wydania	Opis sposobu
Standardowe wydanie certyfikatu dla pierwszego Administratora w podmiocie	Dotyczy Administratorów podmiotów, którzy nie są jeszcze zarejestrowani i w systemie Portal KNF i <b>Centrum Certyfikacji UKNF Portal CA</b> . Subskrybent jest rejestrowany w usłudze katalogowej <b>Centrum Certyfikacji UKNF Portal CA</b> Portalu Komisji Nadzoru Finansowego zgodnie z wewnętrznymi procedurami. Po dokonaniu rejestracji osoba upoważniona, wysyła wniosek o wydanie certyfikatu. W przypadku poprawnej weryfikacji, wniosek zostaje zaakceptowany. <b>Centrum Certyfikacji UKNF Portal CA</b> generuje klucze, wydaje certyfikat i przekazuje użytkownikowi certyfikat w postaci pliku PKCS#12 wraz z dokumentacją stowarzyszoną drogą elektroniczną, w zaszyfowanym pliku. Hasło do pliku jest przekazywane osobnym kanałem komunikacji.

	<p>Hasło do instalacji certyfikatu przekazywane jest przez system Portal KNF na indywidualny adres email użytkownika.</p>
<p>Uproszczone wydanie certyfikatu</p>	<p>Dotyczy subskrybentów, którzy są zarejestrowani w systemie Portalu KNF i usłudze katalogowej <b>Centrum Certyfikacji UKNF Portal CA</b> Urzędu Komisji Nadzoru Finansowego w Warszawie.</p> <p>Użytkownik wysyła wniosek. W przypadku poprawnej weryfikacji, wniosek zostaje zaakceptowany. <b>Centrum Certyfikacji UKNF Portal CA</b> przekazuje użytkownikowi certyfikat w postaci pliku PKCS#12 wraz z dokumentacją stowarzyszoną drogą elektroniczną, w zahasłowanym pliku.</p> <p>Hasło do pliku jest przekazywane osobnym kanałem komunikacji.</p> <p>Hasło do instalacji certyfikatu przesyłane jest przez system Portal na indywidualny adres email użytkownika, zarejestrowany w Portalu.</p>
<p>Obsługa certyfikatów użytkowników merytorycznych w podmiocie przez Administratora podmiotu (dotyczy również innych administratorów w danym podmiocie)</p>	<p>Zarządzanie kontami i certyfikatami użytkowników merytorycznych w podmiotach należy do zadań Administratora w podmiocie. Administrator wysyła żądanie certyfikatu do <b>Centrum Certyfikacji UKNF Portal CA</b> dla Użytkowników merytorycznych podmiotu, innych Administratorów w podmiocie oraz dla siebie. Administrator w podmiocie, pobiera certyfikat z systemu Portal (<b>Centrum Certyfikacji UKNF Portal CA</b> i przekazuje użytkownikowi do instalacji certyfikat w postaci pliku PKCS#12).</p> <p>Hasło do instalacji certyfikatu przesyłane jest przez system Portal KNF na indywidualny adres email użytkownika, zarejestrowany w Portalu KNF.</p>
<p>Obsługa certyfikatów użytkowników merytorycznych technicznych podmiotów utworzonych w celu zapewnienia korespondencji z Powiernikami banków hipotecznych przez Administratora Portalu.</p>	<p>Zarządzanie kontami i certyfikatami użytkowników merytorycznych w technicznych podmiotach utworzonych w celu zapewnienia korespondencji z Powiernikami banków hipotecznych należy do zadań Administratora w Portalu, który w tym przypadku ma konto Administratora w podmiocie. Administrator wysyła żądanie certyfikatu do Centrum Certyfikacji UKNF Portal CA dla Użytkowników merytorycznych podmiotu, innych Administratorów w podmiocie oraz dla siebie. Administrator, pobiera certyfikat z systemu Portal KNF (Centrum Certyfikacji UKNF Portal CA przekazuje użytkownikowi certyfikat w postaci pliku PKCS#12) wraz z dokumentacją stowarzyszoną drogą elektroniczną, w zahasłowanym pliku.</p> <p>Hasło do pliku jest przekazywane osobnym kanałem komunikacji.</p> <p>Hasło do instalacji certyfikatu przesyłane jest przez system Portal KNF na indywidualny adres email użytkownika, zarejestrowany w Portalu KNF.</p>

#### 4.3.2 Powiadomienie subskrybenta o wydaniu certyfikatu przez CA

Wystawiony certyfikat oraz odpowiadający mu klucz prywatny zapisywane są w pliku PKCS#12 i przekazywane są z wykorzystaniem środków komunikacji elektronicznej. Każdorazowe wydanie certyfikatów jest odnotowywane w bazie danych **Centrum**

**Certyfikacji Portalu Komisji Nadzoru Finansowego.** Wydawane certyfikaty są publikowane w repozytorium wewnętrznym.

#### **4.4 Akceptacja certyfikatu**

Subskrybent otrzymujący certyfikat zobowiązany jest do sprawdzenia poprawności zawartych w certyfikacie danych. Należy także sprawdzić, czy klucz publiczny odpowiada posiadanemu kluczowi prywatnemu. W przypadku wystąpienia jakichkolwiek nieprawidłowości, które nie mogą być zaakceptowane przez subskrybenta, należy zgłosić ten fakt w celu natychmiastowego unieważnienia certyfikatu. Jeżeli subskrybent nie ma przeciwwskazań, co do zawartości certyfikatu (zmian można dokonywać w ciągu 3 dni od wystawienia certyfikatu) oznacza to, że certyfikat zostanie zaakceptowany.

##### **4.4.1 Czynności związane z akceptacją certyfikatu**

Subskrybent, który składa wniosek o dostęp do Portalu KNF automatycznie wyraża zgodę na wydanie lub odnowienie certyfikatu.

Brak reklamacji lub użycie certyfikatu do uwierzytelniania do **Portalu Komisji Nadzoru Finansowego** uważane jest za akceptację certyfikatu. Akceptacja jest równoważna z wyrażeniem zgody na zasady zawarte w niniejszym dokumencie oraz w Kodeksie Postępowania Certyfikacyjnego, subskrybent zobowiązuje się przez to do wypełniania obowiązków wynikających z postanowień zawartych w ww. dokumentach.

##### **4.4.2 Publikacja certyfikatu przez CA**

Urząd certyfikacji **UKNF Portal CA** publikuje certyfikat w repozytorium wewnętrznym niezwłocznie po jego wystawieniu.

**UWAGA: Publikowanie certyfikatu nie zależy od uprzedniego zaakceptowania go przez subskrybenta.**

##### **4.4.3 Powiadomienie innych podmiotów o wydaniu certyfikatu przez CA**

Ponieważ certyfikaty służą wyłącznie do uwierzytelniania do systemu Portalu KNF, nie powiadamia się innych podmiotów zewnętrznych o wydaniu certyfikatu.

#### **4.5 Zakres używania pary kluczy i certyfikatów**

##### **4.5.1 Zakres używania klucza prywatnego subskrybenta i certyfikatu**

Klucze i certyfikaty subskrybenta mogą być wykorzystane wyłącznie do uwierzytelniania do **Portalu Komisji Nadzoru Finansowego**.

Subskrybenci:

1. Ponoszą odpowiedzialność za właściwe zrozumienie działania świadczonych usług **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, podstawowych zasad kryptografii i funkcjonowania certyfikatów.
2. Powinni dostarczać do **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** tylko i wyłącznie prawdziwe informacje, bez błędów, utajień lub wieloznacznych sformułowań.
3. Muszą wyrazić zgodę na warunki zawarte w dokumentach Polityki Certyfikacji oraz Kodeksie Postępowania Certyfikacyjnego.

4. Do zarządzania certyfikatami, powinni używać autoryzowanych narzędzi dostarczonych przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.
5. Powinni używać certyfikatów wydanych przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** do celów zgodnych z prawem i przeznaczeniem oraz wytycznymi **Urzędu Komisji Nadzoru Finansowego**.
6. Mogą korzystać tylko i wyłącznie z certyfikatów, których są właścicielami.
7. Zobowiązują się chronić klucz prywatny i hasło po pliku PKCS#12 przed nieautoryzowanym dostępem.
8. Powinni poinformować **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** o ewentualnych zmianach w treści certyfikatów własnych lub o konieczności zmiany treści certyfikatów innych subskrybentów, w przypadku gdy treść ta może być błędna lub niejednoznaczna.
9. Powinni zaprzestać używania certyfikatu, którego zawartość budzi podejrzenia lub zawiera błędy.
10. Powinni natychmiastowo poinformować urząd certyfikacji w przypadku podejrzenia nieprawidłowości w działaniu klucza prywatnego lub jego ewentualnej kompromitacji. W takiej sytuacji niezwłocznie należy zawnioskować o unieważnienie certyfikatu.
11. Powinni zaprzestać używania certyfikatu, którego data ważności została przekroczona lub, co do którego subskrybent podejrzewa naruszenie poufności klucza prywatnego.

#### **4.5.2 Zakres używania klucza publicznego przez podmioty ufające**

Podmioty ufające:

1. Ponoszą odpowiedzialność za właściwe zrozumienie działania **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, podstawowych zasad kryptografii i funkcjonowania certyfikatów.
2. Muszą wyrazić zgodę na warunki zawarte w dokumentach Polityki Certyfikacji oraz Kodeksie Postępowania Certyfikacyjnego.
3. Powinni zweryfikować certyfikaty wydawane przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, włączając w to odpowiedzi z serwera OCSP lub listę certyfikatów unieważnionych (CRL), zgodnie z przyjętymi w **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** zasadami.
4. Powinni ufać i korzystać z certyfikatów wydanych przez urząd certyfikacji **KNF Portal CA** które posiadają aktualną datę ważności, nie są zawieszane, ani odwołane.
5. Powinni każdorazowo oceniać, czy ufać określonemu certyfikatowi wydanemu przez **KNF Portal CA**. Powinni również zwrócić uwagę, czy sytuacja, w której mogliby zaufać certyfikatowi rzeczywiście tego wymaga.
6. Powinni stosować się do reguł i zasad obowiązujących w **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, co do importu oraz eksportu certyfikatów.

#### **4.6 Odnowienie certyfikatu**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie stosuje odnawiania certyfikatów użytkowników Portalu KNF. Zamiast tego, przed wygaśnięciem certyfikatu, generowany będzie nowy certyfikat dla użytkownika i przekazywany osobiście lub z

wykorzystaniem środków komunikacji elektronicznej. Certyfikaty infrastrukturalne odnawiane będą zgodnie z wewnętrznymi procedurami **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

#### **4.7 Aktualizacja klucza certyfikatu**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie stosuje aktualizacji kluczy użytkowników Portalu KNF. Zamiast tego, przed wygaśnięciem certyfikatu, generowany będzie nowy certyfikat dla użytkownika i przekazywany osobiście lub z wykorzystaniem środków komunikacji elektronicznej.

#### **4.8 Modyfikacja certyfikatu**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi modyfikacji certyfikatów.

##### **4.8.1 Okoliczności modyfikacji certyfikatu**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi modyfikacji certyfikatów.

##### **4.8.2 Kto może wnioskować o modyfikację certyfikatu**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi modyfikacji certyfikatów.

##### **4.8.3 Przetwarzanie wniosków o modyfikację certyfikatów**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi modyfikacji certyfikatów.

##### **4.8.4 Powiadomienie subskrybenta o wydaniu zmodyfikowanego certyfikatu**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi modyfikacji certyfikatów.

##### **4.8.5 Czynności związane z akceptacją zmodyfikowanego certyfikatu**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi modyfikacji certyfikatów.

##### **4.8.6 Publikacja zmodyfikowanego certyfikatu przez CA**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi modyfikacji certyfikatów.

#### **4.8.7 Powiadomienie innych podmiotów o wydaniu certyfikatu przez CA**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi modyfikacji certyfikatów.

#### **4.9 Unieważnienie i zawieszenie certyfikatu**

Unieważnienie jest jedną z najważniejszych procedur w **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**. Czas, w którym certyfikaty są unieważnianie odgrywa istotną rolę. Po unieważnieniu uznaje się, że certyfikat stracił ważność, czyli jest w stanie unieważnienia. Unieważnienie nie może być anulowane.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi zawieszania certyfikatów

##### **4.9.1 Okoliczności unieważnienia certyfikatu**

Certyfikaty mogą zostać unieważnione z następujących powodów:

1. Ujawnienie klucza prywatnego lub utrata kontroli nad kluczem prywatnym.
2. Naruszanie przez subskrybenta certyfikatu zasad Polityki Certyfikacji.
3. Dezaktualizacja informacji w certyfikacie.
4. Wydanie certyfikatu niezgodnego z zasadami Polityki Certyfikacji.
5. Zakończenie prowadzenia usług certyfikacyjnych przez główny urząd certyfikacji (unieważnia się wszystkie certyfikaty wydane przez ten urząd oraz certyfikat samego urzędu certyfikacji)
6. Bezpośrednie zagrożenie wiarygodności certyfikatów spowodowane przełamaniem systemu zabezpieczeń **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.
7. Inne przyczyny zaburzające wypełnianie postanowień Polityki Certyfikacji, np. kłęski żywiołowe, awaria systemów komputerowych.
8. Zastąpienie certyfikatu innym wydanym według innego szablonu, np. zmieniono długość kluczy, lub polityki aplikacji zawarte w certyfikacie.

##### **4.9.2 Kto może wnioskować o unieważnienie certyfikatu**

O unieważnienie mogą także wnioskować następujące strony:

1. Właściciel certyfikatu.
2. Administratorzy **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.
3. Osoba, która zauważyła rażące nieprawidłowości w działaniu certyfikatu.
4. Inne osoby upoważnione, których role obejmują możliwość wnioskowania o unieważnienie.

##### **4.9.3 Procedura dla wniosku o unieważnienie certyfikatu**

Unieważnienie certyfikatu odbywa się na podstawie złożonego przez upoważnioną osobę wniosku. Szczegółowa procedura opisana jest w Kodeksie Postępowania Certyfikacyjnego.

##### **4.9.4 Czas odroczenia prośby o unieważnienie certyfikatu**

Wszystkie wnioski o unieważnienie są traktowane priorytetowo. **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie definiuje czasu odroczenia prośby o unieważnienie certyfikatu. Zakłada się jednak możliwość wystąpienia pewnych opóźnień np. z

przyczyn technicznych, maksymalny czas odroczenia w takich przypadkach wynosi 24 godziny.

#### **4.9.5 Czas, w którym CA musi przetworzyć wniosek o unieważnienie**

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** przetwarza wnioski o unieważnienie w trybie natychmiastowym. Dopuszczalne są niewielkie opóźnienia wynikające z przyczyn technicznych. Przez opóźnienia należy rozumieć czas, jaki minie pomiędzy momentem otrzymania wniosku o unieważnienie a jego rozpatrzeniem. Nie należy mylić tego okresu czasu z okresem publikowania listy certyfikatów unieważnionych CRL.

#### **4.9.6 Obowiązek sprawdzania unieważnionych certyfikatów przez podmioty ufające**

Podmioty ufające muszą przed użyciem określonego certyfikatu wydanego przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** sprawdzić za każdym razem, czy certyfikat jest poprawny. Brane pod uwagę powinny być głównie: odpowiedzi z serwera OCSP i lista certyfikatów unieważnionych CRL. W przypadku zaistnienia jakichkolwiek wątpliwości, nie należy korzystać z certyfikatu.

#### **4.9.7 Częstotliwość publikowania list CRL (jeśli konieczne)**

Publikacja list CRL następuje co **21 dni** oraz po unieważnieniu certyfikatu.

#### **4.9.8 Maksymalne opóźnienie publikacji list CRL (jeśli konieczne)**

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** gwarantuje, że maksymalne okresy zwłoki dotyczące przetwarzania wniosków o umieszczenie certyfikatu na liście certyfikatów unieważnionych CRL, nie przekraczają okresów, które zakłóciłyby prowadzenie działalności przez subskrybentów oraz zaburzyły bezpieczeństwo informacji.

#### **4.9.9 Dostępność sprawdzenia bieżącego statusu unieważnienia**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** oferuje usługę weryfikacji certyfikatu w czasie rzeczywistym za pomocą protokołu OCSP. Protokół OCSP umożliwia uzyskanie informacji o statusie certyfikatu bez potrzeby pobierania stałej listy CRL. Serwer OCSP może zwrócić odpowiedzi: poprawny, unieważniony lub nieznan.

#### **4.9.10 Wymagania dotyczące bieżącego sprawdzania unieważnienia**

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nakłada obowiązek na stronę ufającą weryfikacji statusu certyfikatu on-line za pomocą protokołu OCSP.

#### **4.9.11 Inne dostępne formy zgłaszania stanu unieważnienia**

Nie dotyczy.

#### **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**

korzysta tylko z metody umieszczania informacji o certyfikatach unieważnionych opartej na liście CRL oraz odpowiedziach z serwera OCSP.

#### **4.9.12 Wymogi specjalne odnośnie kompromitacji klucza**

W sytuacji, gdy subskrybent podejrzewa kompromitację klucza prywatnego własnego certyfikatu, powinien:

1. Natychmiastowo zaprzestać używania certyfikatu.



2. Zainicjalizować procedurę wnioskowania o unieważnienie certyfikatu.

#### **4.9.13 Okoliczności zawieszenia certyfikatu**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi zawieszania certyfikatów.

#### **4.9.14 Kto może wnioskować o zawieszenie**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi zawieszania certyfikatów.

#### **4.9.15 Procedura dla wniosków o zawieszenie**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi zawieszania certyfikatów.

#### **4.9.16 Ograniczenia, co do okresu zawieszenia**

Nie dotyczy.

**Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie oferuje usługi zawieszania certyfikatów.

### **4.10 Usługi związane ze statusem certyfikatu**

#### **4.10.1 Charakterystyka funkcjonalności**

Zarówno certyfikaty, jak i listy certyfikatów odwołanych CRL publikowane są w ogólnodostępnym repozytorium dostępnym pod adresem:

**<http://pki.knf.gov.pl/pki/uknfportalca2019.crl>**

Subskrybenci i strony ufające mają możliwość sprawdzenia statusu certyfikatu także za pomocą serwera OCSP. Informacje znajdujące się w repozytorium obejmują:

1. Certyfikat głównego urzędu **Centrum Certyfikacji Komisji Nadzoru Finansowego**.
2. Certyfikat **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.
3. Aktualizowaną listę certyfikatów unieważnionych CRL.

#### **4.10.2 Dostępność usług**

Usługi certyfikacji **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** działają w trybie 24x7 (całą dobę przez 7 dni w tygodniu). **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie może zagwarantować, że usługi te będą udostępniane w takim trybie przez cały czas, wynika to z braku możliwości przewidzenia zdarzeń losowych, na które **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie ma wpływu.

#### **4.10.3 Dodatkowe funkcje**

Nie dotyczy.

#### 4.11 Czas wygaśnięcia

Subskrypcja certyfikatu kończy się, gdy certyfikat nie został odnowiony przed końcową datą wygaśnięcia. Na wniosek subskrybenta, subskrypcja może zakończyć się wcześniej. Poniższe tabele przedstawiają czasy życia certyfikatów urzędów certyfikacji oraz czasy życia certyfikatów wystawianych przez poszczególne urzędy certyfikacji.

**Tabela 6 Czasy życia certyfikatów CA**

Nazwa CA	Czas życia certyfikatu	Czas odnowienia	Generowanie nowych kluczy co
UKNF Portal CA	5 lat	Przed upływem 4 lat ważności SubCA	Podczas odnowienia certyfikatu

**Tabela 7 Czasy życia certyfikatów wydanych przez CA**

Nazwa CA	Maksymalny czas życia certyfikatów wydawanych przez CA
UKNF Portal CA	1 rok

#### 4.12 Deponowanie i odtworzenie kluczy

Nie dotyczy.

**Centrum Certyfikacji Portalu Urzędu Komisji Nadzoru Finansowego** nie stosuje mechanizmu deponowania i odtwarzania kluczy

### 5 Zabezpieczenia fizyczne i organizacyjne

Zabezpieczenia stosowane w **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** są zgodne z wymaganiami **Urzędu Komisji Nadzoru Finansowego**.

Informacje na temat stosowanych w **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** zabezpieczeń zostały umieszczone w Kodeksie Postępowania Certyfikacyjnego.

### 6 Zabezpieczenia techniczne

Zabezpieczenia techniczne stosowane w **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** są zgodne z wymaganiami **Urzędu Komisji Nadzoru Finansowego** i dobierane na podstawie szacowania ryzyka.

Informacje na temat stosowanych w **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** zabezpieczeń zostały umieszczone w Kodeksie Postępowania Certyfikacyjnego.

### 7 Profile certyfikatów, list CRL i OCSP

Certyfikaty wydawane przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, odpowiedzi z serwera OCSP oraz listy CRL są wystawiane zgodnie ze zdefiniowanymi i zatwierdzonymi przez **Urząd Komisji Nadzoru Finansowego** profilami.

Opis profili został umieszczony w Kodeksie Postępowania Certyfikacyjnego.

## **8 Audyt i inne sposoby oceny**

Audyty i przeglądy systemu prowadzone są zgodnie z zasadami obowiązującymi w **Urzędzie Komisji Nadzoru Finansowego**.

## **9 Pozostałe zagadnienia i kwestie prawne**

### **9.1 Opłaty**

Nie dotyczy.

### **9.2 Odpowiedzialność finansowa**

Nie dotyczy.

### **9.3 Poufność informacji**

**Urząd Komisji Nadzoru Finansowego gwarantuje**, że do publicznej wiadomości mogą być udostępniane tylko te informacje, które są publicznie dostępne w certyfikacie.

Dane, które subskrybenci wpisują we wnioskach o wydanie certyfikatu są podawane tylko dla wiedzy wybranych komórek organizacyjnych **Urzędu Komisji Nadzoru Finansowego** i nie zostaną ujawnione innym podmiotom, z wyjątkiem sytuacji, w których obowiązek ich ujawnienia wynika z powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych.

#### **9.3.1 Zakres informacji poufnych**

Informacje poufne opisane w niniejszym dokumencie nie są tym samym, co informacje poufne w znaczeniu ustawy o ochronie informacji niejawnych. Słowo „poufne” należy rozumieć w sposób tradycyjny jako „udostępniane tylko niewielu osobom, wymagające dyskrecji”.

Informacje, które **Urząd Komisji Nadzoru Finansowego** uzyskuje podczas wykonywania czynności certyfikacyjnych są uważane za informacje poufne. **Urząd Komisji Nadzoru Finansowego** zobowiązuje się do odpowiedniej ochrony tych informacji.

Jakiegokolwiek ujawnienie danych subskrybenta wymaga pisemnej zgody ich właściciela lub prawomocnego nakazu sądowego, chyba, że obowiązek ich ujawnienia wynika z powszechnie obowiązujących przepisów prawa.

Zgodnie z wewnętrznymi regulacjami **Urzędu Komisji Nadzoru Finansowego**, ochronie podlegają następujące informacje:

1. Uzyskane od subskrybentów podczas czynności administracyjnych np. treści wniosków o wydanie i unieważnienie certyfikatów. Wyjątki znajdują się w rozdziale: 9.3.2 „Informacje będące poza zakresem poufności”.
2. Dzienniki bezpieczeństwa.
3. Plany działań awaryjnych.
4. Informacje o zabezpieczeniach sprzętu oraz oprogramowania.
5. Informacje dotyczące administracji usługami certyfikacyjnymi.
6. Inne informacje, które z punktu widzenia **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** są uznawane za informacje wrażliwe.

### **9.3.2 Informacje będące poza zakresem poufności**

Z uwzględnieniem regulacji zawartych w rozdziale 9.3.1 „Zakres informacji poufnych”, wszystkie pozostałe informacje uważane są za jawne. W szczególności do informacji jawnych należą:

1. Certyfikat subskrybenta.
2. Informacje zawarte w repozytorium.

Subskrybenci akceptujący certyfikaty wydane przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** automatycznie wyrażają zgodę na upublicznienie tych informacji.

### **9.3.3 Odpowiedzialność za ochronę informacji poufnych**

Obowiązek ochrony informacji poufnych wynika z przepisów wewnętrznych oraz obowiązujących na terenie Rzeczypospolitej Polskiej przepisów.

**Urząd Komisji Nadzoru Finansowego** ponosi odpowiedzialność za ochronę informacji subskrybentów, podmiotów ufających, jak i informacji, których poufność jest regulowana wewnętrznymi regulacjami **Urzędu Komisji Nadzoru Finansowego**.

Użytkownicy, którym została powierzona informacji poufna, są za nią odpowiedzialni i zobowiązują się do zachowania tajemnicy przy użyciu dostępnych im środków. Jakikolwiek ujawnienie informacji poufnych prowadzi do konsekwencji służbowych i prawnych.

## **9.4 Ochrona danych osobowych**

Dane osobowe są przetwarzane przez **Komisję Nadzoru Finansowego** w związku z działaniem **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** na podstawie przepisów prawa powszechnie obowiązującego w tym w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

## **9.5 Prawo do własności intelektualnej**

**Urząd Komisji Nadzoru Finansowego** zastrzega sobie prawo do roszczeń sądowych wynikających z naruszenia własności intelektualnej instytucji. Poprzez dobra intelektualne, do których **Urząd Komisji Nadzoru Finansowego** zastrzega sobie prawo, rozumie się dobra nie posiadające postaci materialnej. Stanowią one wynik twórczości naukowej, wynalazczej oraz artystycznej pracowników **Urzędu Komisji Nadzoru Finansowego**. Za dobra intelektualne uważa się używane przez **Urząd Komisji Nadzoru Finansowego**:

1. znaki towarowe oraz handlowe.
2. patenty.
3. znaki graficzne.
4. licencje.
5. wynalazki i projekty.
6. inne.

## **9.6 Rękojmie i gwarancje**

**Urząd Komisji Nadzoru Finansowego** gwarantuje, że informacje umieszczane w certyfikatach wydawanych w ramach działania **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** są zgodne ze stanem faktycznym.

Potwierdzenie tego stanu realizowane jest poprzez dokładne sprawdzenie tożsamości subskrybenta wnoszącego o wydanie certyfikatu.

## **9.7 Zastrzeżenia gwarancji**

**Urząd Komisji Nadzoru Finansowego** zapewnia, że konfiguracja zarówno urzędów certyfikacji, jak i całej infrastruktury klucza publicznego została wykonana z największą starannością. Jednakże fakt ten nie gwarantuje, że **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** będzie w stanie w pełni zabezpieczyć się przed działaniami, które są od **Urzędu Komisji Nadzoru Finansowego** niezależne. Uprawnienia z tytułu gwarancji nie obejmują prawa subskrybenta do dochodzenia roszczeń z tytułu poniesienia strat w wyniku nieprawidłowego funkcjonowania **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

Przerwy techniczne lub błędy w działaniu usług certyfikacyjnych nie mogą powodować roszczeń subskrybentów, czy podmiotów ufających.

## **9.8 Ograniczenia odpowiedzialności**

**Urząd Komisji Nadzoru Finansowego** nie ponosi odpowiedzialności za świadome działania użytkowników mające na celu obniżenie poziomu bezpieczeństwa **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

**Urząd Komisji Nadzoru Finansowego** nie ponosi odpowiedzialności za błędy w funkcjonowaniu urzędów certyfikacji powstałe w wyniku:

1. błędów oprogramowania, na które **Urząd Komisji Nadzoru Finansowego** nie miał wpływu.
2. nieprawidłowości w działaniu sprzętu wspomagającego infrastrukturę klucza publicznego.
3. działań ludzkich niezależnych od **Urzędu Komisji Nadzoru Finansowego**.
4. innych losowych zdarzeń, na które **Urząd Komisji Nadzoru Finansowego** nie miał wpływu.

## **9.9 Odszkodowania**

Nie dotyczy.

**Urząd Komisji Nadzoru Finansowego** nie wypłaca odszkodowań z tytułu nieprawidłowo realizowanych usług certyfikacji.

## **9.10 Okres obowiązywania i wygaśnięcie**

### **9.10.1 Okres obowiązywania**

Niniejszy dokument Polityki Certyfikacji obowiązuje od momentu umieszczenia go w ogólnodostępnym repozytorium pod adresem <https://bip.knf.gov.pl/> i pozostaje w mocy, aż do ogłoszenia kolejnej wersji Polityki Certyfikacji.

### 9.10.2 Wygaśnięcie

Dokument polityki Certyfikacji pozostaje w mocy do czasu aż:

1. Będzie istniał co najmniej jeden aktualny certyfikat wydany przez urząd certyfikacji, zgodnie z zaleceniami w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.
2. Nie zostanie zastąpiony nowszą wersją.

### 9.10.3 Efekty wygaśnięcia

Wygaśnięcie Polityki Certyfikacji pozostawia w mocy prawo do własności intelektualnej oraz zachowuje poufność wszystkich informacji zgromadzonych w ramach świadczenia usług **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**

### 9.11 Powiadomienia indywidualne oraz kontakt z uczestnikami

Polityka Certyfikacji nie zawiera konkretnych ustaleń, co do powiadomień indywidualnych oraz kontaktu z uczestnikami. W przypadku składania wniosków przez subskrybentów formy kontaktu zostały opisane w rozdziałach poświęconych określonym czynnościom.

### 9.12 Poprawki

Zmiany w Polityce Certyfikacji mogą wynikać z:

1. zauważonych błędów.
2. uaktualnień samej Polityki Certyfikacji lub uaktualnień wynikających ze znaczących zmian infrastrukturalnych wpływających na treść niniejszego dokumentu.
3. sugestii ze strony zainteresowanych stron.

Propozycje wprowadzania zmian do istniejącej Polityki Certyfikacji mogą zgłaszać:

1. audytorzy.
2. instytucje prawne.
3. Administrator Bezpieczeństwa Informacji, Administrator Systemów Centrum Certyfikacji, Administrator CA oraz inni pracownicy **Centrum Certyfikacji Portalu Urzędu Komisji Nadzoru Finansowego**.
4. subskrybenci **Centrum Certyfikacji Portalu Urzędu Komisji Nadzoru Finansowego** oraz podmioty ufające.
5. eksperci z zakresu zabezpieczeń systemów informatycznych.

Propozycje zmian powinny być przesyłane pocztą elektroniczną na adres [knf@knf.gov.pl](mailto:knf@knf.gov.pl).

### 9.13 Ustalenia, co do rozstrzygania sporów

Przedmiotem rozstrzygania sporów mogą być:

1. rozbieżności w interpretacji Polityki Certyfikacji.
2. zażalenia dotyczące działania certyfikatu wydanego przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**.

Osoby, które chcą złożyć zażalenie na usługi certyfikacji udostępniane przez **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego**, czy na nieprawidłowości w treści Polityki Certyfikacji lub też inne elementy wchodzące w skład infrastruktury klucza publicznego **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** powinny poinformować **Urząd Komisji Nadzoru Finansowego** o tym fakcie. Informacja powinna

zawierać dokładny opis przedmiotu sporu. UKNF zobowiązuje się do ustosunkowania do zastrzeżeń w terminie 14 dni.

#### **9.14 Obowiązujące prawa i regulacje**

Postanowienia niniejszej Polityki Certyfikacji pozostają w zgodzie z właściwymi przepisami polskiego prawa.

#### **9.15 Zgodność ze stosownymi przepisami prawa**

Postanowienia niniejszej Polityki Certyfikacji pozostają w zgodzie z właściwymi przepisami ipolskiego prawa.

#### **9.16 Pozostałe ustalenia**

##### **9.16.1 Całość porozumienia**

Niniejsza Polityka Certyfikacji i wszystkie inne dokumenty do niej dołączone, czyli dokumenty, o których wyraźnie wspomina się w treści oraz dokumenty towarzyszące (np. instrukcje dla użytkowników i specyfikacje), stanowią całość porozumienia stron w przedmiotowym zakresie i zastępują wszystkie terminy i przepisy zawarte w innych dokumentach tj. politykach, regulacjach i ustaleniach wewnętrznych wymienianych przez strony.

##### **9.16.2 Cesja**

Nie istnieją żadne, porozumienia lub przedsięwzięcia, inne niż te wyraźnie określone w dokumencie Polityki Certyfikacji.

##### **9.16.3 Rozdzielność postanowień umowy**

Jeżeli którekolwiek z postanowień niniejszego dokumentu jest nieważne, nie będzie to miało wpływu na obowiązywanie jakichkolwiek innych postanowień niniejszego dokumentu.

##### **9.16.4 Egzekwowanie**

Nie dotyczy.

##### **9.16.5 Siła wyższa**

Odpowiedzialność **Urzędu Komisji Nadzoru Finansowego** za świadczenie usług **Centrum Certyfikacji Portalu Komisji Nadzoru Finansowego** nie obejmuje odpowiedzialności za skutki zdarzeń wynikających z działania siły wyższej. Działanie siły wyższej obejmuje zarówno trudne do przewidzenia zjawiska naturalne (na przykład trzęsienia ziemi, powodzie, huragany) jak i działania ludzkie, niezależne bezpośrednio od **Urzędu Komisji Nadzoru Finansowego** (na przykład wojny, ataki terrorystyczne, nacjonalizacja, strajki), poważne problemy techniczne takie jak awarie sieci energetycznej czy sieci telekomunikacyjnych oraz inne zjawiska o podobnym charakterze lub skutkach.

#### **9.17 Pozostałe ustalenia**

Nie dotyczy.