# Dokumentacja Centrum Certyfikacji
# CEPS 2.0

| | |
|---|---|
| Tytuł dokumentu: | POLITYKA CERTYFIKACJI DLA PODMIOTÓW KORZYSTAJĄCYCH Z SYSTEMU INFORMATYCZNEGO CEPS 2.0 |
| Wersja: | **1.0** |
| Data wersji: | **2025-11-28** |

Historia dokumentu

| Wersja | Data | Uwagi | Autor |
|---|---|---|---|
| 0.1 | 2023-10-12 | Wersja inicjalna | Kmuk Łukasz |
| 0.2 | 2024-01-17 | 1. Zmieniono długość klucza<br>2. Zmieniono CEPS na CEPS 2.0 | COI |
| 0.3 | 2024-02-12 | Zmiana nazw DN | COI |
| 1.0 | 2025-11-28 | Zmiany dotyczące Root'a | COI |

# Spis treści

# 1. Wstęp

## 1.1. Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji (CC), działające w strukturach organizacyjnych MC, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla systemu Centralnej Ewidencji Pojazdów Służbowych (CEPS 2.0) w zakresie generowania certyfikatów i kluczy dla wszystkich Subskrybentów, tj. przedstawicieli instytucji wskazanych w art. 73 ust. 3 ustawy prawo o ruchu drogowym oraz urządzeń wchodzących w skład infrastruktury CEPS 2.0.

W związku z tym, że dokument zawiera również uregulowania szczegółowe w zakresie objętym polityką certyfikacji, pełni on jednocześnie rolę regulaminu certyfikacji.

O ile nie zaznaczono inaczej, stosowne zapisy niniejszego dokumentu „Polityki Certyfikacji dla podmiotów korzystających z systemu informatycznego CEPS 2.0" dotyczą wszystkich opisywanych podsystemów.

Postanowienia niniejszej polityki certyfikacji są zgodne z wymaganiami nałożonymi rozporządzeniem Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (D. U. 2020, poz. 399).

Struktura dokumentu została oparta na dokumencie RFC 3647 *"Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework".*

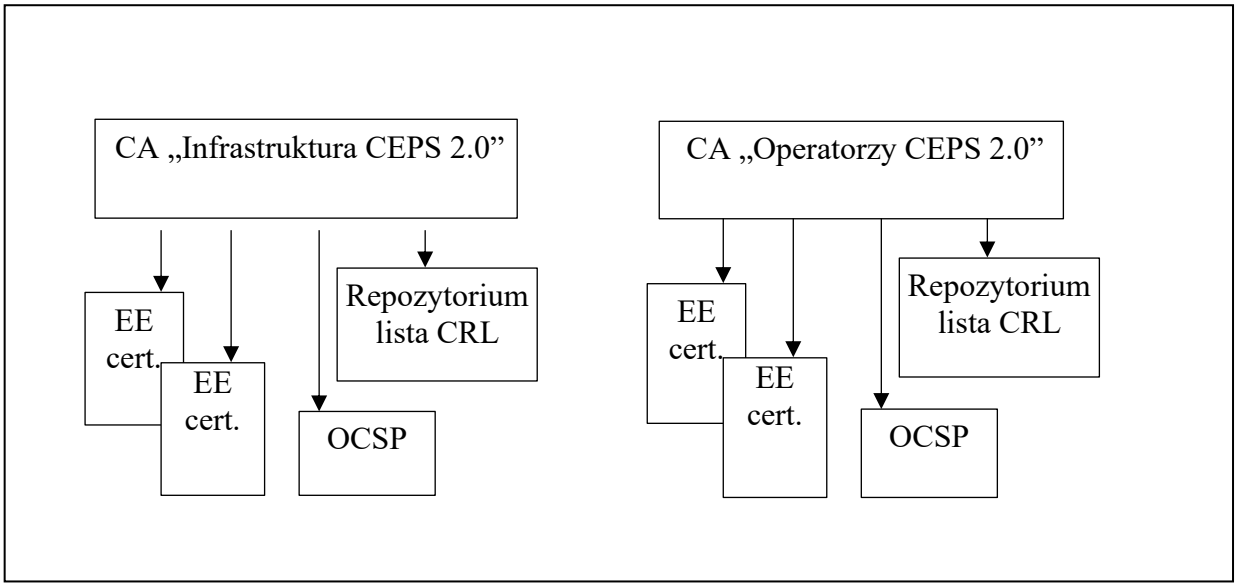
W rozdziale 1.6 zamieszczono słownik pojęć stosowanych w dokumencie.

## 1.2. Identyfikator polityki certyfikacji

| | |
|---|---|
| Nazwa polityki | Polityka certyfikacji dla podmiotów korzystających z systemu CEPS 2.0 |
| Kwalifikator polityki | Brak |
| Wersja polityki | 1.0 |
| Numer OID (ang. *Object Identifier*) | 0.4.0.2042.1.3<br><br>itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) lcp (3) |

## 1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

Niniejsza polityka certyfikacji realizowana jest przez CC, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla CEPS 2.0. CC realizuje polityki certyfikacji za pomocą tzw. podsystemów certyfikacji. Usługi certyfikacyjne (wg rozporządzenia eIDAS *usługi zaufania*) dla CEPS 2.0 realizowane są w ramach dwóch podsystemów certyfikacji (CA), co obrazuje poniższy rysunek:




Każdy podsystem certyfikacji posiada swój własny urząd certyfikacji (CA; ang. *Certification Authority*), identyfikowany za pomocą swojej własnej nazwy wyróżniającej (pole *issuer* w stosownych certyfikatach) – patrz rozdz. 7.1.3. W każdym podsystemie publikowana jest lista CRL lub realizowana jest usługa OCSP (ang. *Online Certificate Status Protocol*).

Wszystkim Subskrybentom, w ramach niniejszej polityki certyfikacji, certyfikaty wystawiane są na podstawie decyzji, porozumień lub umów z MC oraz przepisów prawa określających w szczególności zasady zachowania poufności informacji oraz zakres i zasady odpowiedzialności stron.

Subskrybentami usług certyfikacyjnych realizowanych zgodnie z niniejszą polityką certyfikacji są użytkownicy działający w ramach CEPS 2.0 oraz systemy i urządzenia wykorzystywane w ramach CEPS 2.0, przy czym w przypadku systemów i urządzeń pojęcie *Subskrybent* obejmuje również administratora (tzw. sponsora) odpowiedniego systemu lub urządzenia.

W ramach niniejszej polityki certyfikacji Subskrybentami są:

W podsystemie „**Infrastruktura CEPS**” wydawane są certyfikaty na potrzeby funkcjonowania systemu i wewnętrznej komunikacji modułów w ramach systemu CEPS 2.0.

W podsystemie „**Operatorzy CEPS**” osoby realizujące zadania na rzecz podmiotów, które na mocy przepisów prawa są uprawnione do zasilania i dostępu do danych gromadzonych w CEPS 2.0 oraz administratorzy systemu informatycznego CEPS 2.0.

W ramach systemu CC obowiązują określone dla realizowanej polityki certyfikacji procedury i zasady oraz dla każdego podsystemu certyfikacji stworzono specyficzne profile nazw i certyfikatów. CA generują pary kluczy kryptograficznych osobno dla każdego podsystemu certyfikacji, służące do składania poświadczeń (pieczęci) elektronicznych pod certyfikatami i listami unieważnionych certyfikatów.

Subskrybenci CEPS 2.0 uzyskują certyfikaty w ramach niniejszej polityki certyfikacji kontaktując się z CC COI, którego dane kontaktowe podane są w rozdziale **Błąd! Nie można odnaleźć źródła odwołania.**.

Personel Centrum Certyfikacji prowadzi obsługę wniosków o dostęp do CEPS 2.0 w zakresie świadczenia usług certyfikacyjnych, a w szczególności zlecania generowania certyfikatów, wydawania przygotowanych nośników zawierających certyfikaty, przyjmowania zleceń unieważnienia.

Wystawione w ramach niniejszej polityki certyfikaty powinny jednoznacznie identyfikować Subskrybenta. Gdy certyfikat nie jest imienny (nie jest wystawiony dla konkretnej osoby, której imię i nazwisko widnieje w certyfikacie), to wymagane jest, aby Subskrybent zapewnił rozliczalność użycia kluczy prywatnych związanych z wystawionymi w niniejszej polityce certyfikatami poprzez:

- ewidencję powiązań pomiędzy certyfikatami a nośnikami kluczy kryptograficznych lub urządzeniami zawierającymi klucze prywatne związane z tymi certyfikatami,
- ewidencję użycia nośników kluczy kryptograficznych lub urządzeń przez pracowników Subskrybenta[1],
- ewidencję powiązań pomiędzy podpisanymi elektronicznie komunikatami w systemie CEPS 2.0 a pracownikami Subskrybenta upoważnionymi do pracy w systemie.

## 1.4. Zakres zastosowań

W ramach niniejszej polityki certyfikacji generowane są:

1. Certyfikaty do weryfikowania podpisów elektronicznych składanych przez Subskrybenta pod poleceniami przesyłanymi do systemu CEPS 2.0.
2. Certyfikaty służące do zabezpieczenia transmisji danych w komunikacji pomiędzy Subskrybentem a systemem CEPS 2.0.
3. Certyfikaty do identyfikowania Subskrybenta łączącego się z systemem CEPS 2.0.

Certyfikaty Subskrybentów wystawione w ramach niniejszej polityki certyfikacji nie mogą być używane do innych celów niż określone powyżej.

[1] przez pracowników należy także rozumieć funkcjonariuszy, żołnierzy lub inne osoby upoważnione przez Subskrybenta do użycia nośników kluczy kryptograficznych lub urządzeń zawierających klucze prywatne związane z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami

## 1.5. Zasady administrowania polityką certyfikacji

Niniejsza polityka certyfikacji została opracowana na potrzeby systemu CEPS 2.0. Wszelkie zmiany niniejszej polityki certyfikacji, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymagają zatwierdzenia przez Gestora systemu.

### 1.5.1 Punkty kontaktowe

Punktem kontaktowym dla obsługi wszelkich spraw związanych z realizacją niniejszej polityki certyfikacji przez CC jest:

**Centrum Certyfikacji**
**Centralny Ośrodek Informatyki**
**ul. Gdańska 47/49**
**90-729 Łódź**

**e-mail: cc.coi@cyfra.gov.pl**
**tel. (42) 253 54 71**

**W przypadku kierowania korespondencji przez ePUAP należy ją kierować na adres ePUAP Centralnego Ośrodka Informatyki.**

## 1.6. Słownik używanych terminów i akronimów

W niniejszym dokumencie następujące sformułowania użyte będą w wymienionym poniżej znaczeniu:

| Pojęcie | Opis |
|---|---|
| Ustawa | Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173, ze zm.). |
| Rozporządzenie | Rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (D. U. 2020, poz. 399, ze zm.) |
| MC | Ministerstwo Cyfryzacji |
| CEPS 2.0 | Centralna Ewidencja Pojazdów Służbowych |
| Subskrybent | Pracownicy (lub żołnierze/funkcjonariusze) jednostek wymienionych w art. 73 ust. 3 „Prawa o ruchu drogowym” , albo system lub urządzenie, otrzymujące certyfikaty zgodnie z niniejszą polityka certyfikacji. Pojęcie to obejmuje również administratora systemu lub urządzenia (tzw. sponsora urządzenia). |
| Gestor systemu | Dyrektor COI, któremu na podstawie umowy z dnia 31sierpnia 2023 r. pomiędzy Ministrem Cyfryzacji a COI powierzono zarządzanie zasobem. Gestor ponosi odpowiedzialność kierowniczą przed Ministrem właściwym ds. informatyzacji, za nadzór nad eksploatacją, rozwojem, utrzymaniem, korzystaniem, bezpieczeństwem i dostępem do zasobu. |

| Pojęcie | Opis |
|---|---|
| CC | Centrum Certyfikacji – system certyfikacji prowadzony pod kontrolą Gestora; system CC składa się z podsystemów certyfikacji realizujących polityki certyfikacji i posługujących się odrębnymi kluczami do generowania certyfikatów i list unieważnionych certyfikatów. |
| CC COI | Centrum Certyfikacji Centralnego Ośrodka Informatyki – komórka COI odpowiedzialna za merytoryczną obsługę wniosków certyfikacyjnych i kontakt z Subskrybentem. Dane adresowe są określone w rozdz. 1.5.1. |
| Certyfikat | Elektroniczne zaświadczenie za pomocą, którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby (lub urządzenia) składającej podpis elektroniczny, i które umożliwiają identyfikację tej osoby/urządzenia. |
| Zaświadczenie certyfikacyjne | Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do danego podsystemu certyfikacji CC, i które umożliwiają identyfikację tego podsystemu. Zaświadczenia certyfikacyjne stosowane w ramach niniejszej polityki certyfikacji mają postać self-issued certyfikatów X.509. Są typu „link certyfikat" (tzw. zakładkowy certyfikat *old*with*new* i *new*with*old* wg RFC 4210) oraz typu „self-signed certyfikat" (tzw. samopodpisany klucz urzędu CA; *new*with*new*). |
| DN | (ang. *Distinguished Name*) nazwa wyróżniająca zgodna z zaleceniami zdefiniowanymi w ITU z serii X.500. Jednoznacznie identyfikuje ona Subskrybenta usług certyfikacyjnych i podmiot wydający certyfikaty. |
| Domena | Pewien podzbiór Subskrybentów, którzy posiadają identyczny zbiór atrybutów (określony w strukturze DN) zawartych w nazwie certyfikatu (pole *subject*). |
| PR | Punkt Rejestracji - element systemu odpowiedzialny za wprowadzanie zgłoszeń certyfikacyjnych do systemu, przygotowywanie i personalizowanie nośników kluczy kryptograficznych oraz obsługę zgłoszeń unieważnienia certyfikatów. |
| Inspektor ds. rejestracji | Osoba upoważniona do pracy w PR, posiadająca klucze i certyfikaty upoważniające do wykonywania w podsystemie certyfikacji operacji przypisanych do PR. |
| Klucze infrastruktury | Klucze kryptograficzne stosowane do innych celów niż składanie lub weryfikacja zaawansowanego podpisu elektronicznego używane wewnętrznie w CC, a w szczególności klucze stosowane do zapewnienia integralności rejestrów zdarzeń, klucze do szyfrowania przesyłanych lub przechowywanych danych. |
| Osoba weryfikująca certyfikat | Osoba fizyczna, prawna lub urządzenie, które wykorzystuje klucz publiczny zawarty w certyfikacie. |
| Punkt zaufania | Najbardziej zaufany urząd certyfikacji, któremu ufa Subskrybent lub strona ufająca. Certyfikat tego urzędu jest pierwszym certyfikatem w każdej ścieżce certyfikacji, zbudowanej przez Subskrybenta lub stronę ufająca. Wybór punktu zaufania jest zwykle narzucany przez politykę certyfikacji, według której funkcjonuje podmiot świadczący usługi certyfikacyjne. |
| Lista CRL | Lista unieważnionych certyfikatów i zaświadczeń certyfikacyjnych. |
| Ścieżka certyfikacji | Uporządkowany ciąg certyfikatów, prowadzący od certyfikatu punktu zaufania, wybranego przez weryfikującego, aż do weryfikowanego certyfikatu, utworzony w celu weryfikacji certyfikatu. Ścieżka certyfikacji spełnia następujące warunki:<br>• dla każdego certyfikatu Cert(x) należącego do ścieżki certyfikacji {Cert(1), Cert(2), ..., Cert(n-1)} podmiot certyfikatu Cert(x) jest wydawcą certyfikatu Cert(x+1),<br>• certyfikat Cert(1) jest wydany przez urząd certyfikacji (punkt zaufania), któremu ufa weryfikator,<br>• Cert(n) jest weryfikowanym certyfikatem. |

| Pojęcie | Opis |
|---|---|
| Informatyczny nośnik danych (nośnik) | Pamięć flash, płyta CD/DVD, karta kryptograficzna. |
| OCSP | (ang. *Online Certificate Status Protokol*) Protokół zgodny z RFC 6960, za pomocą którego można uzyskać informację o statusie wskazanego certyfikatu. |
| LDAP | Baza danych przechowująca informacje o Subskrybentach dostępna za pomocą protokołu LDAP[2]. |
| ITSM Atmosfera. | System do rejestracji wniosków i zgłoszeń. |

[2] *Lightweight Directory Access Protocol* (LDAP) – protokół przeznaczony do korzystania z usług katalogowych, bazujący na standardzie X.500

# 2. Zasady dystrybucji i publikacji informacji

W ramach systemu certyfikacji działa Repozytorium. Jest ono dostępne za pośrednictwem protokołów LDAP (serwer LDAP).

CC zapewnia dystrybucję wystawionych certyfikatów i list unieważnionych certyfikatów w następujący sposób:

1. Informacje o wydaniu certyfikatu (DN) publikowane są na serwerze LDAP.
2. Listy CRL publikowane są na serwerze CA.

Certyfikaty publikowane są niezwłocznie po ich wystawieniu, nie później jednak niż 72 godziny od momentu wystawienia.

Listy CRL publikowane są niezwłocznie po ich wystawieniu. Wystawienie listy CRL następuje nie później niż po 1 godzinie od unieważnienia certyfikatu. Listy CRL są wystawiane w odstępach nie dłuższych niż 24 godziny. Ważność list CRL określona jest na 48 godzin.

Dostęp do serwera LDAP jest ograniczony do podmiotów działających w centrali systemu CEPS 2.0. Nie przewiduje się szerszego udostępnienia zawartości serwera.

Szczegółowych informacji dla Subskrybentów o adresach i zasadach dostępu do Repozytorium udziela CC COI.

# 3. Identyfikacja i uwierzytelnienie

Niniejszy rozdział opisuje zasady identyfikacji i uwierzytelnienia Subskrybentów.

## 3.1. Struktura nazw przydzielanych Subskrybentom

W poniższych rozdziałach znajdują się struktury nazw wyróżniających zapisywanych do pola *subject* stosowanych EE certyfikatów.

### 3.1.1 Podsystem „Infrastruktura CEPS”

#### 3.1.1.1 Domena *Systemy i urządzenia CEPS*

Kraj (countryName) C = PL

Nazwa organizacji (organizationName) O = CEPS

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <SYSTEMY / URZADZENIA>

Nazwa powszechna (commonName) CN = <NAZWA HOSTA / IP>

#### 3.1.1.2 Domeny w środowisku testowym

Dla celów testowych struktura DN jest identyczna jak opisana powyżej za wyjątkiem pola *Nazwa organizacji* (organizationName), gdzie O = CEPS-TEST

#### 3.1.1.3 Zawartość pól

Pola *countryName, organizationName* oraz *organizationalUnitName* zawierają wartości stałe określone w pkt 3.1.1.1– 3.1.1.2.

Pole *commonName* = *NAZWA HOSTA / IP* zawiera nazwę hosta lub adres IP Subskrybenta.

#### 3.1.1.4 Unikalność nazw Subskrybentów

Nie dopuszcza się, aby Subskrybent posiadał certyfikat z danymi, które nie identyfikują go w sposób jednoznaczny. Każdy Subskrybent musi posiadać certyfikat umożliwiający jego jednoznaczną identyfikację. Unikalność danych Subskrybenta jest rozumiana jako unikalny dla każdego Subskrybenta zestaw danych składający się z wartości pola *commonName* (pozostałe pola mają wartość stałą).

### 3.1.2 Podsystem „Operatorzy CEPS”

#### 3.1.2.1 Domena *Operatorzy CEPS*

Kraj (countryName) C = PL

Nazwa organizacji (organizationName) O = CEPS

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = < Rodzaj instytucji>

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Pełna nazwa podmiotu>

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Pełna nazwa podmiotu c.d.> (opcjonalnie)

Numer seryjny (serialNumber) SN = <PESEL lub KOD>

Nazwa powszechna (commonName) CN = <Imię i nazwisko> (opcjonalnie)

**Zawartość pól**:

Pola *countryName, organizationName* zawierają wartości stałe określone w pkt. 3.1.2.1.

Pole *organizationalUnitName = Rodzaj instytucji* wskazuje typ podmiotu Subskrybenta. Jest to pole słownikowe wybierane przez Subskrybenta z listy rozwijanej w formularzu wniosku certyfikacyjnego, na początkowym etapie wypełniania formularza elektronicznego.

Pole *organizationalUnitName = Pełna nazwa podmiotu i Pełna nazwa podmiotu c.d.* zawiera nazwę Subskrybenta. Jest to pole wypełniane przez Subskrybenta we wniosku certyfikacyjnym. Długość pola na wniosku to 2 linie po 64 znaki.

Pole s*erialNumber = pole* zawiera PESEL operatora lub KOD nadany przez Służbę. Jest to pole wypełniane przez Subskrybenta we wniosku certyfikacyjnym.

Pole *commonName* = pole opcjonalne, wypełniane tylko w sytuacji użycia nr PESEL. Imię i nazwisko zawiera imię i nazwisko operatora (tzw. certyfikat imienny). Pole jest wypełniane przez Subskrybenta.

### 3.1.2.2 Domeny w środowisku testowym

Dla celów testowych struktura DN jest identyczna jak opisana powyżej za wyjątkiem

pola *Nazwa organizacji* (organizationName), gdzie O = CEPS-TEST.

### 3.1.2.3 Unikalność nazw Subskrybentów

Nie dopuszcza się, aby Subskrybent posiadał certyfikat z danymi, które nie identyfikują go w sposób jednoznaczny. Każdy Subskrybent musi posiadać certyfikat umożliwiający jego jednoznaczną identyfikację. Unikalność danych Subskrybenta jest rozumiana jako unikalny dla każdego Subskrybenta zestaw danych składający się z wartości pól:

- *organizationalUnitName* (dwa lub trzy wystąpienia pola),
- *serialNumber,*
- *commonName* (pole opcjonalne).

## 3.2. Rejestracja i uwierzytelnienie Subskrybenta

Podrozdział opisuje sposoby udowodnienia posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie oraz sposoby uwierzytelnienia Subskrybentów w procesie wnioskowania o certyfikaty, jak również przy odnawianiu certyfikatów oraz ich unieważnianiu.

### 3.2.1 Sposoby uwierzytelnienia Subskrybentów przy początkowej rejestracji i wystawianiu pierwszego certyfikatu

Rejestracja Subskrybentów oraz wygenerowanie im certyfikatów odbywa się na podstawie pisemnego zapotrzebowania (tzw. wniosek certyfikacyjny; patrz rozdz. 4.1), podpisanego przez osoby upoważnione do reprezentowania Subskrybenta.

Wniosek zawiera m.in. imię i nazwisko osoby uprawnionej odpowiednio do:

1. Odbioru nośników z kluczami i certyfikatami oraz numerów PIN/haseł.
2. Zgłaszania potrzeby unieważnienia certyfikatów.
3. Kontaktów z CC COI.

Potwierdzenie tożsamości Subskrybenta następuje w ramach procedury administracyjnej związanej z obsługą danego wniosku.

W przypadku osobistego kontaktu z PR, potwierdzenie tożsamości Subskrybenta następuje w oparciu o jeden z dokumentów potwierdzający tożsamość (dowód osobisty, paszport, karta stałego pobytu) wskazany we wniosku certyfikacyjnym. W przypadku innych niż uprawnione do reprezentowania Subskrybenta osób kontaktujących się z CC COI lub PR, wymagane jest upoważnienie potwierdzające możliwość reprezentowania danego Subskrybenta przez daną osobę. Upoważnienie potwierdzające możliwość reprezentowania Subskrybenta przez daną osobę powinny być podpisane przez osoby uprawnione do reprezentowania Subskrybenta.

### 3.2.2 Sposoby udowodnienia posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie

Pary kluczy mogą być generowane na następujące sposoby:

1. W PR przez Inspektora ds. rejestracji bezpośrednio przed procesem generowania certyfikatów. W takim przypadku w naturalny sposób jest zapewnione, że Subskrybent, po otrzymaniu nośnika kluczy kryptograficznych, posiada klucz prywatny związany z kluczem publicznym umieszczonym w certyfikacie.
2. Przez Subskrybenta. W takim przypadku dowodem posiadania klucza prywatnego jest podpisane tym kluczem i dostarczone do PR zgłoszenie certyfikacyjne, zgodne z formatem PKCS#10.

### 3.2.3 Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów

Wystawienie Subskrybentowi certyfikatu dla nowej pary kluczy (tzw. wymiana certyfikatu) odbywa się według tych samych reguł co wystawienie pierwszego certyfikatu.

W celu zachowania ciągłości pracy Subskrybent powinien wystąpić o wymianę/odnowienie certyfikatu przesyłając wniosek certyfikacyjny, jeżeli jest to wymagane wraz z nośnikiem kryptograficznym lub zgłoszeniem certyfikacyjnym, w okresie ważności certyfikatu dotychczasowego, z odpowiednim wyprzedzeniem, nie mniejszym niż miesiąc i nie większym niż 2 miesiące przed końcem jego ważności.

### 3.2.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia certyfikatu

Prawo do unieważnienia certyfikatu mają osoby (fizyczne i/lub prawne) wpisane do certyfikatu, osoby uprawnione do reprezentowania Subskrybenta w kontaktach z CC COI wskazane we wniosku certyfikacyjnym oraz Gestor, jak również przełożeni tych osób – patrz rozdz. 4.9.2.

Pisemne żądanie unieważnienia certyfikatu musi być przekazane do CC COI (rozdz. 1.5.1); w sytuacjach awaryjnych dopuszczalny jest kontakt telefoniczny lub mail'owy.

Żądanie unieważnienia certyfikatu powinno zawierać co najmniej:

1. Nazwę wydawcy certyfikatu (pole *issuer*), czyli wskazanie podsystemu certyfikacji – patrz rozdz. 1.3 (tym samym dodatkowo wskazanie na system „produkcyjny" lub „testowy" – atrybut OU).
2. Pewne atrybuty nazwy właściciela certyfikatu (pole *subject*), tj.:

   **Domena „Infrastruktura CEPS"**

   a) *commonName*.

   **Domena „Operatorzy CEPS"**

   a) wartości wszystkich wystąpień atrybutu *Nazwa jednostki organizacyjnej* zawartych w certyfikacie;
   b) *serialNumber*: PESEL lub KOD;
   c) *commonName* (imię i nazwisko; atrybut podawany tylko w przypadku certyfikatów imiennych, czyli gdy *serialNumber* zawiera PESEL).
3. O ile jest to możliwe – numer seryjny certyfikatu.

Powinien być podany również powód unieważnienia certyfikatu.

# 4. Cykl życia certyfikatu – wymagania operacyjne

## 4.1. Wniosek certyfikacyjny

Każdy certyfikat wystawiany w ramach niniejszej polityki certyfikacji (z wyjątkiem certyfikatów Inspektorów ds. rejestracji oraz certyfikatów kluczy infrastruktury dla wewnętrznych zastosowań CC) jest wystawiany w oparciu o tzw. wniosek certyfikacyjny.

Każdy wniosek (bez względu na wybór podsystemu, którego dotyczy) musi zostać wydrukowany, podpisany przez Wnioskującego i opatrzony pieczęcią jednostki organizacyjnej jednoznacznie wskazującą na wnioskujący podmiot. Następnie podpisany oryginał wniosku należy przesłać do CC COI, którego dane kontaktowe podane są w rozdziale **Błąd! Nie można odnaleźć źródła odwołania.**.

Przed przesłaniem pierwszego wniosku certyfikacyjnego zalecane jest skontaktowanie się z CC COI (1.5.1) w celu ustalenia poprawności wyboru i wypełnienia wniosku.

W zależności od podsystemu certyfikacji wniosek certyfikacyjny zawiera różny zbiór danych, co zostało opisane w poniższych podrozdziałach 4.1.1 i 4.1.2.

### 4.1.1 Podsystem „Infrastruktura CEPS”

Nie dopuszcza się wystawienia Subskrybentowi wielu certyfikatów (na różne pary kluczy) w oparciu o jeden wniosek certyfikacyjny.

Zgodnie z formularzem ze strony www, wniosek certyfikacyjny zawiera w szczególności następujące dane:

- wskazanie podstawy prawnej wnioskowania o certyfikat (przepis prawa, umowa, porozumienie, decyzja),
- nazwa polityki certyfikacji, której dotyczy wniosek (czyli „Polityka certyfikacji dla podmiotów korzystających z systemu informatycznego CEPS 2.0” podsystem Infrastruktura CEPS),
- rodzaj wniosku (nowy użytkownik, dodatkowy certyfikat, odnowienie certyfikatu/recertyfikacja, unieważnienie certyfikatu),
- wskazanie środowiska systemu CEPS 2.0 (produkcyjne lub testowe),
- dane osoby reprezentującej podmiot (Subskrybenta),
- dane osoby upoważnionej do kontaktu z CC COI w sprawach związanych z certyfikatami, w tym adres e-mail,
- miejscowość i datę wypełnienia wniosku,
- pieczęć i podpis,

Do wniosku należy dołączyć zgłoszenie certyfikacyjne w formacie PKCS#10, zawierające w polu *subject* nazwę hosta lub adres IP Subskrybenta (atrybut *commonName*).

### 4.1.2 Podsystem „Operatorzy CEPS”

Nie dopuszcza się wystawienia Subskrybentowi wielu certyfikatów imiennych (na różne pary kluczy) w oparciu o jeden wniosek certyfikacyjny.

Zgodnie z formularzem ze strony www wniosek certyfikacyjny zawiera w szczególności następujące dane:

- wskazanie interesariusza,
- wskazanie podstawy prawnej wnioskowania o certyfikat (przepis prawa, umowa, porozumienie, decyzja),
- nazwa polityki certyfikacji, której dotyczy wniosek (czyli „Polityka certyfikacji dla podmiotów korzystających z systemu informatycznego CEPS 2.0” podsystem Operatorzy CEPS),
- wskazanie środowiska systemu CEPS 2.0 (produkcyjne lub testowe),
- pełna nazwa podmiotu (zgodna z wpisem w bazie GUS),
- REGON (zgodny z wpisem w bazie GUS),
- dane operatora (imię, nazwisko, PESEL) lub KOD,
- adres podmiotu (Subskrybenta),
- dane osoby reprezentującej podmiot (Subskrybenta),
- dane osoby upoważnionej do kontaktu z CC COI w sprawach związanych z certyfikatami, w tym adres e-mail,
- miejscowość i datę wypełnienia wniosku,
- pieczęć i podpis,

Do wniosku należy dołączyć opcjonalnie nośnik typu karta kryptograficzna lub zgłoszenie certyfikacyjne w formacie PKCS#10.

Ponadto należy dołączyć informację potwierdzającą, że osoba operatora, identyfikująca się imieniem i nazwiskiem oraz nr PESEL, albo kodem (KOD) użytkownika, jest osobą uprawnioną do dostępu do danych poufnych i do pomieszczenia dedykowanego do systemu CEPS 2.0. Informacja ta musi być podpisana przez osobę reprezentującą podmiot (instytucję).

## 4.2. Przetwarzanie wniosków i zgłoszeń certyfikacyjnych

Realizacja wniosku następuje w terminie nie dłuższym niż 20 dni roboczych liczonych od dnia wpływu wniosku do CC COI (1.5.1).

W przypadku wezwania Subskrybenta do uzupełnienia braków formalnych we wniosku termin ten wydłuża się o dni oczekiwania na uzupełnienie wykazanych braków (nie dłużej niż 14 dni kalendarzowych).

CC COI po otrzymaniu wniosku ewidencjonuje otrzymaną korespondencję oraz ewentualnie nośnik, następnie skanuje wniosek i rejestruje w ITSM Atmosfera. W kolejnym kroku CC COI weryfikuje zawartość merytoryczną oraz kompletność dokumentacji. Kompletne zgłoszenie powinno zawierać:

- prawidłowo wypełniony, podstemplowany oraz podpisany wniosek,
- upoważnienie do złożenia wniosku – jeśli wniosek jest składany przez osobę upoważnioną przez reprezentanta podmiotu,
- nośnik – jeśli wniosek wymaga dołączenia nośnika,
- zgłoszenie certyfikacyjne – jeżeli wniosek jest na certyfikat w pliku.

Pozytywnie zweryfikowany wniosek wraz z nośnikiem (jeżeli został dołączony) lub zgłoszeniem certyfikacyjnym przekazywany jest do PR w celu utworzenia / odnowienia / unieważnienia / zmiany danych certyfikatu.

Po zrealizowaniu wniosku, PR wysyła do użytkownika listem poleconym nośnik z certyfikatem (tj. kartę kryptograficzną) i kopertę z kodem PIN (w osobnych przesyłkach). Możliwy jest również odbiór osobisty.

Certyfikaty ze zgłoszeń certyfikacyjnych przekazywane są drogą elektroniczną poprzez system ITSM Atmosfera.

W przypadku braków formalnych bądź konieczności uzupełnienia wniosku wzywa się Subskrybenta poprzez stosowną informację z systemu ITSM Atmosfera (na adres e-mailowy podany we wniosku) do dostarczenia niezbędnych dokumentów, nośników bądź informacji w czasie nie dłuższym niż 14 dni kalendarzowych od dnia powiadomienia Interesanta o konieczności uzupełnienia wniosku.

Wnioski niezasadne lub te, które ze względu braków formalnych lub błędnych danych zawartych we wniosku zostają odrzucone, kończą obsługę po stronie Centrum Certyfikacji, o czym Subskrybent zostaje poinformowany z systemu ITSM Atmosfera (na adres e-mailowy podany we wniosku).

## 4.3. Wystawienie certyfikatu

Przed wystawieniem certyfikatu CC COI analizuje wniosek certyfikacyjny (patrz rozdz. 4.2), a po jego zaakceptowaniu przekazuje do realizacji.

Certyfikaty są wystawiane na podstawie zlecenia przygotowywanego i uwierzytelnianego elektronicznie przez Inspektora ds. rejestracji w PR lub dostarczonego przez Subskrybenta. Natychmiast po wystawieniu są nagrywane na nośniki i/lub przekazywane wybranym kanałem dystrybucji (patrz rozdz. 4.2) do osób upoważnionych wskazanych we wniosku.

## 4.4. Akceptacja certyfikatu

Za akceptację certyfikatu uznaje się pierwsze użycie certyfikatu przez Subskrybenta.

## 4.5. Korzystanie z pary kluczy i certyfikatu

Subskrybent jest zobowiązany do przestrzegania postanowień, wymagań i procedur opisanych w niniejszej polityce certyfikacji.

W przypadku certyfikatów imiennych (pole *subject* certyfikatu zawiera imię i nazwisko) Subskrybent musi zapewnić, że tylko on będzie się nim posługiwał. W przypadku pozostałych certyfikatów Subskrybent musi zapewnić system ewidencji użycia nośników kluczy kryptograficznych związanych z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami służącymi do składania podpisów elektronicznych pod podpisywanymi poleceniami dla systemu CEPS 2.0. Zasady te powinny obejmować co najmniej:

1. Kontrolę tożsamości osób upoważnionych do używania nośników kluczy kryptograficznych, przez osobę upoważnioną do ich wydawania.
2. Prowadzenie ewidencji nośników kluczy kryptograficznych, określającej numery certyfikatów związanych z zawartymi na tych nośnikach kluczami.
3. Prowadzenie ewidencji wydanych nośników kluczy kryptograficznych, zawierającej co najmniej:
    a) datę i godzinę wydania lub zwrotu nośnika,
    b) identyfikator nośnika,
    c) imię i nazwisko, a w razie potrzeby również inne dane osoby odbierającej nośnik (np. numer służbowy),
    d) podpis osoby odbierającej nośnik – w przypadku wydania kluczy, podpis osoby odbierającej nośnik – w przypadku zwrotu nośnika.
4. Przechowywanie ewidencji przez odpowiedni okres, umożliwiający skuteczne działania uprawnionych organów w przypadku wystąpienia nieprawidłowości w operacjach wykonywanych w systemie CEPS 2.0 przez osoby upoważnione przez Subskrybenta.

Subskrybent jest zobowiązany do wykorzystywania certyfikatu i związanego z nim klucza prywatnego wyłącznie w ramach systemu CEPS 2.0.

Subskrybent jest zobowiązany do przechowywania kluczy prywatnych związanych z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami wyłącznie na nośnikach kluczy kryptograficznych lub urządzeniach spełniających techniczne wymagania dla komponentów technicznych określone w ustawie i towarzyszących jej aktach wykonawczych.

Subskrybent jest zobowiązany do niezwłocznego zgłaszania do CC COI potrzeby unieważnienia certyfikatu w przypadku ujawnienia lub zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej polityki certyfikacji.

Subskrybent jest zobowiązany do zniszczenia kluczy prywatnych związanych z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami w sytuacji, gdy:

- zaprzestaje on korzystania z systemu CEPS 2.0 lub
- unieważnia on certyfikat związany z tym kluczem lub
- wycofuje daną parę kluczy z użycia.

Za zniszczenie klucza prywatnego uznaje się jego logiczne usunięcie z nośnika kluczy kryptograficznych lub z urządzenia.

Podmiotem działającym w oparciu o certyfikaty wystawione w ramach niniejszej polityki certyfikacji może być wyłącznie MC, które na podstawie tych certyfikatów uwierzytelnia Subskrybentów. Inne podmioty, które decydują się działać w oparciu o certyfikaty wystawione w ramach niniejszej polityki ponoszą pełną, bezwarunkową odpowiedzialność za skutki takich działań, niezależnie od wszelkich działań lub braku działań podejmowanych przez CC, również wtedy, gdy działania lub brak działań ze strony CC są niezgodne z niniejszą polityką certyfikacji.

## 4.6. Odnowienie certyfikatu (*Renewal*)

Nie jest dopuszczalne ponowne wystawienie certyfikatu dla tej samej pary kluczy (*Renewal*).

## 4.7. Wymiana certyfikatu połączona z wymianą pary kluczy (*Re-key*)

Wystawienie certyfikatu dla nowej pary kluczy (w szczególności w sytuacji, gdy nie istnieje ważny certyfikat w ramach niniejszej polityki certyfikacji) odbywa się według procedur określonych w rozdziałach 4.1-4.4.

Nie dopuszcza się wystawienia certyfikatu dla pary kluczy, dla której poprzednio wystawiony certyfikat został unieważniony, niezależnie od przyczyny unieważnienia. Subskrybent zobowiązany jest do przedsięwzięcia takich środków, które zapewnią, iż w kolejnych nadsyłanych przez niego zgłoszeniach certyfikacyjnych nie występuje klucz publiczny, którego certyfikat wystawiony w ramach niniejszej polityki certyfikacji został unieważniony.

## 4.8. Zmiana treści certyfikatu

Zmiana treści certyfikatu wymaga wystawienia nowego certyfikatu (zawierającego nową treść) i unieważnienia dotychczasowego certyfikatu (zawierającego starą treść). Wystawienie nowego certyfikatu odbywa się według procedur określonych w rozdziałach 4.1-4.4.

## 4.9. Unieważnienie certyfikatu

Unieważnienie ma ściśle określony wpływ na certyfikaty oraz obowiązki posługującego się nim Subskrybenta (w tym administratora urządzenia). Natychmiast po unieważnieniu certyfikatu należy uznać, że certyfikat stracił ważność (jest w stanie unieważnienia). Podobnie w przypadku certyfikatów urzędów certyfikacji, anulowanie ważności tego rodzaju certyfikatu oznacza cofnięcie jego posiadaczowi prawa do wydawania certyfikatów, ale nie wpływa na ważność

certyfikatów wydanych przez tenże urząd certyfikacji w okresie, gdy jego certyfikat był ważny, o ile nie doszło do kompromitacji klucza urzędu – patrz rozdz. 5.7.1 i 5.7.2.

### 4.9.1 Okoliczności unieważnienia certyfikatu

Podstawową przyczyną unieważnienia certyfikatu jest fakt utraty (lub samo podejrzenie takiej utraty) kontroli nad kluczem prywatnym, będącym w posiadaniu Subskrybenta (w tym administratora danego urządzenia) lub też rażące naruszanie przez Subskrybenta zasad niniejszej polityki certyfikacji.

Unieważnianie certyfikatu może mieć miejsce w następujących okolicznościach:

- gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się (np. nastąpiła zmiana nazwiska pracownika),
- ilekroć klucz prywatny związany z kluczem publicznym zawartym w certyfikacie lub nośnik, na którym jest przechowywany został ujawniony lub istnieje uzasadnione podejrzenie, że będzie ujawniony[3]; procedura unieważniania certyfikatu jest wówczas przeprowadzana na wniosek Subskrybenta,
- jeżeli Subskrybent zaprzestaje korzystania z systemu CEPS 2.0 w wyniku zmian w prawie lub w innych, podobnych sytuacjach,
- o unieważnienie certyfikatu może wystąpić Subskrybent lub Gestor systemu,
- certyfikat może być unieważniony, jeżeli zmianie ulega polityka certyfikacji i konieczne jest zaprzestanie używania dotychczasowych certyfikatów ze względu na sprzeczność z postanowieniami nowej polityki certyfikacji,
- w przypadku zakończenia działalności przez urząd certyfikacji unieważnia się wszystkie certyfikaty wydane przez ten urząd przed upływem deklarowanego terminu zakończenia działalności, a także certyfikat samego urzędu certyfikacji,
- gdy klucz prywatny lub bezpieczeństwo systemu komputerowego urzędu certyfikacji zostały ujawnione w sposób, który bezpośrednio zagraża wiarygodności certyfikatów,
- gdy zaistnieją inne przyczyny opóźniające lub uniemożliwiające Subskrybentowi wypełnianie postanowień niniejszej polityki certyfikacji, powstałe wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa Subskrybent lub oficjalnych działań rządu lub jego agend.

Postępowanie Subskrybenta w przypadku unieważniania certyfikatu opisano w rozdziale 3.2.4.

Za skutki użycia klucza prywatnego związanego z certyfikatem, do czasu wystawienia przez odpowiedni podsystem pierwszej listy CRL zawierającej informację o unieważnieniu tego certyfikatu, odpowiada Subskrybent.

### 4.9.2 Kto może żądać unieważnienia certyfikatu

Następujące podmioty mogą zgłaszać żądanie unieważnienia certyfikatu Subskrybenta:

---

3 Ujawnienie klucza prywatnego oznacza: (1) nieuprawniony dostęp lub podejrzenie nieuprawnionego dostępu do klucza prywatnego, (2) zagubienie lub podejrzenie zagubienia klucza prywatnego, (3) kradzież lub podejrzenie kradzieży klucza prywatnego, (4) przypadkowe zniszczenie klucza prywatnego.

- Subskrybent będący podmiotem unieważnianego certyfikatu (w tym odpowiedni administrator systemu lub urządzenia),
- autoryzowany przedstawiciel Gestora; dotyczy to w szczególności przypadku unieważniania certyfikatu urzędu certyfikacji, wystawionego przez urząd, który reprezentuje ten autoryzowany przedstawiciel,
- przełożony Subskrybenta (w tym administratora urządzenia) lub osoba do tego upoważniona.

### 4.9.3 Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

CC COI gwarantuje, że maksymalne okresy zwłoki[4] w przetwarzaniu wniosków o unieważnienie certyfikatów nie przekraczają okresów, które w znaczący sposób utrudniłyby prowadzenie działalności przez Subskrybenta lub stronę ufającą.

Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem usługi weryfikacji statusu certyfikatu, natychmiast po dopuszczalnym okresie zwłoki w unieważnieniu certyfikatu.

Fakt unieważnienia certyfikatu odnotowywany jest w bazach danych odpowiedniego podsystemu certyfikacji. Na liście certyfikatów unieważnionych (CRL) lub w odpowiednim tokenie (odpowiedzi) OCSP unieważniony certyfikat zostanie umieszczony zgodnie z przyjętym w CC cyklem publikowania takich list/tokenów OCSP.

### 4.9.4 Częstotliwość publikowania list CRL

Nowa lista CRL dot. certyfikatów osób fizycznych, prawnych, systemów i urządzeń publikowana jest w Repozytorium okresowo (patrz rozdz. 2) oraz po każdym unieważnieniu certyfikatu.

### 4.9.5 Maksymalne opóźnienie w publikowaniu CRL

Od momentu unieważnienia do opublikowania nowej listy CRL nie może upłynąć więcej niż 1 godzina.

Publikacja nowej listy nie może nastąpić później niż jej koniec ważności (patrz rozdz. 2).

### 4.9.6 Dostępne formy ogłaszania unieważnień certyfikatów

Obie metody, tj. listy CRL i/lub tokeny OCSP są stosowane w każdym podsystemie certyfikacji.

W każdym podsystemie certyfikacji odpowiedni urząd CA dokumentuje uzasadnienie unieważnienia poprzez umieszczenie kodu powodu (przyczyny) unieważnienia (jeśli został podany) na liście CRL i/lub tokenach OCSP. W przypadku kodu *unspecified* nie umieszcza się

4 Przez dopuszczalny okres zwłoki należy rozumieć maksymalny dozwolony czas, jaki minie pomiędzy momentem otrzymania wniosku o unieważnienie a momentem zakończenia jego rozpatrywania, odnotowania w bazach urzędu certyfikacji i odesłania decyzji wnioskodawcy. Czasu tego nie należy mylić z okresem publikowania list CRL.

go w rozszerzeniu *cRLReason*, a zamiast tego odpowiedni wpis na liście CRL lub tokenie OCSP nie zawiera tego rozszerzenia.

W przypadku naruszenia ochrony (ujawnienia) kluczy prywatnych urzędów certyfikacji funkcjonujących w ramach CC COI informacja o tym jest umieszczana natychmiast na listach CRL oraz informowani są Subskrybenci tego podsystemu, np. poprzez email.

### 4.9.7 Wymaganie weryfikacji unieważnień online

Nie ma wymagania stosowania usługi OCSP w pewnych okolicznościach – oba mechanizmy: lista CRL lub token OCSP mogą być stosowane zamiennie. Przy wydawaniu tokenów OCSP stosowane są terminy analogiczne, jak dla listy CRL.

## 4.10. Sprawdzanie statusu certyfikatu

Informację o statusie certyfikatów wydanych przez CC COI w każdym z podsystemów można uzyskać w oparciu o listy CRL publikowane za pośrednictwem usługi katalogowej LDAP lub serwera WWW (HTTP), albo za pomocą usługi OCSP.

## 4.11. Powierzanie i odtwarzanie kluczy prywatnych

Nie dopuszcza się powierzania kluczy prywatnych Subskrybentów. Nie jest możliwe odtwarzanie kluczy prywatnych Subskrybentów w przypadku ich utraty lub niedostępności.

# 5. Zabezpieczenia organizacyjne, operacyjne i fizyczne

## 5.1. Zabezpieczenia fizyczne

Szczegółowe procedury i zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa systemu CEPS 2.0.

## 5.2. Zabezpieczenia proceduralne

Szczegółowe procedury i zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa systemu CEPS 2.0.

## 5.3. Zabezpieczenia osobowe

Szczegółowe procedury i zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa systemu CEPS 2.0.

## 5.4. Procedury rejestrowania zdarzeń

Szczegółowe procedury i zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa systemu CEPS 2.0.

## 5.5. Archiwizacja zapisów

Szczegółowe procedury i zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa systemu CEPS 2.0.

## 5.6. Wymiana pary kluczy podsystemu certyfikacji

Wymiana pary kluczy podsystemu certyfikacji może następować w planowych terminach (przed upływem ważności dotychczasowego samopodpisanego zaświadczenia certyfikacyjnego) lub w przypadku wykrycia zwiększonego ryzyka utraty klucza prywatnego (np. na skutek uszkodzenia niektórych nośników klucza prywatnego przechowujących dane niezbędne do odtworzenia klucza prywatnego w stosowanym schemacie podziału sekretu).

Nie dopuszcza się wystawiania nowych samopodpisanych zaświadczeń certyfikacyjnych dla dotychczasowej pary kluczy podsystemu certyfikacji.

Planowa wymiana pary kluczy podsystemu certyfikacji powinna nastąpić nie później niż 2 lata przed końcem okresu ważności dotychczasowego samopodpisanego zaświadczenia certyfikacyjnego.

Procedura planowej wymiany pary kluczy podsystemu certyfikacji nie powoduje konieczności wymiany certyfikatów Subskrybentom.

Postępowanie w przypadku wymiany pary kluczy podsystemu certyfikacji jest następujące:

- CC MC z odpowiednim wyprzedzeniem informuje zainteresowane podmioty o terminie planowanej wymiany kluczy
- CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne i nową listę CRL;
- nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu CEPS 2.0, które tego wymagają, i w taki sposób aby akceptowane były również certyfikaty Subskrybentów poświadczone poprzednim, kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły powinny traktować oba samopodpisane zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania lub, że moduły powinny traktować tylko nowe samopodpisane zaświadczenie certyfikacyjne jako punkt zaufania i posiadać dostęp do zakładkowego zaświadczenia certyfikacyjnego zawierającego dotychczasowy klucz publiczny podsystemu certyfikacji poświadczony nowym kluczem prywatnym podsystemu certyfikacji);
- CC przekazuje Subskrybentom nowe samopodpisane zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne w sposób zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych (o ile to możliwe w ramach protokołów dostępu do systemu CEPS 2.0, w pozostałych przypadkach w sposób uzgodniony z Subskrybentem; dotyczy to przede wszystkim zaświadczenia certyfikacyjnego *new*with*new*, gdyż autentyczność pozostałych zaświadczeń jest zapewniana poprzez ścieżkę certyfikacji rozpoczynającą się od punktu zaufania, czyli klucza publicznego CC),
- po wygenerowaniu nowego samopodpisanego zaświadczenia certyfikacyjnego (*new*with*new* wg RFC 4210) listy CRL są podpisywane tylko nowym kluczem urzędu CC.

## 5.7. Postępowanie po ujawnieniu lub utracie klucza prywatnego podsystemu certyfikacji

Przez ujawnienie klucza prywatnego podsystemu certyfikacji należy rozumieć sytuację, w której nieuprawniona osoba uzyskała możliwość wykorzystywania tego klucza w sposób niezgodny z niniejszą polityką certyfikacji. Procedury obowiązujące przy ujawnieniu klucza należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie ujawnienia klucza.

W przypadku zaistnienia sytuacji, w której nastąpiło podejrzenia naruszenia lub naruszenie poufności, integralności bądź dostępności klucza prywatnego podsystemu certyfikacji, należy podjąć czynności mające na celu:

1. Zgłoszenie incydentu zgodnie z polityką bezpieczeństwa CEPS 2.0.
2. Identyfikację okoliczności i osób mających wpływ na zaistnienie nieprawidłowości.
3. Zebranie i zabezpieczenie materiału dowodowego.
4. Wyciągnięcie wniosków, przedstawienie i realizację zaleceń minimalizujących możliwość zaistnienia podobnych sytuacji w przyszłości.
5. Pociągnięcie osób odpowiedzialnych za zaistniałe nieprawidłowości do odpowiedzialności dyscyplinarnej i/lub karnej.

### 5.7.1 Postępowanie po ujawnieniu klucza prywatnego podsystemu certyfikacji

Wykrycie ujawnienia klucza prywatnego podsystemu certyfikacji lub uzasadnione podejrzenie takiego ujawnienia powoduje następujące, niezwłocznie podejmowane działania:

- Gestor systemu zawiadamia pisemnie lub email'em Administratorów CEPS 2.0 o zaistniałej sytuacji oraz postępuje zgodnie z zapisami polityki bezpieczeństwa CEPS 2.0,
- CC tworzy, w oparciu o skompromitowany klucz (o ile ma do niego dostęp), listę CRL unieważniającą wszystkie ważne certyfikaty oraz zaświadczenia certyfikacyjne, w tym samopodpisane zaświadczenia certyfikacyjne, które zostały wcześniej poświadczone skompromitowanym kluczem;
- administratorzy modułów systemu CEPS 2.0 usuwają wszystkie samopodpisane zaświadczenia certyfikacyjne (i ewentualnie zakładkowe zaświadczenia certyfikacyjne) związane z kluczami prywatnymi tego podsystemu certyfikacji, z tych modułów systemu CEPS 2.0, gdzie występują jako tzw. punkty zaufania;
- Gestor systemu zawiadamia wszystkich Subskrybentów o zaistniałej sytuacji;
- CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Inspektorów ds. rejestracji i certyfikaty kluczy infrastruktury;
- nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu CEPS 2.0, które tego wymagają;
- PR, działając w uzgodnieniu z Subskrybentami, na podstawie posiadanych wniosków certyfikacyjnych generuje nowe certyfikaty zastępujące wszystkie dotychczas wystawione certyfikaty; jeżeli konieczne jest wygenerowanie nowych par kluczy wówczas wymagane jest przeprowadzenie standardowego postępowania określonego w rozdziałach 4.1-4.4;
- PR dostarcza nowe certyfikaty i samopodpisane zaświadczenie certyfikacyjne (*new*with*new* wg RFC 4210) w sposób uzgodniony z Subskrybentem, zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych;
- dotychczasowy (ujawniony) klucz prywatny jest niszczony (sposób niszczenia jest określony w procedurach operacyjnych).

Jeśli baza danych podsystemu certyfikacji jest wiarygodna pomimo ujawnienia klucza, decyzją Gestora systemu nowe certyfikaty można wygenerować w oparciu o certyfikaty znajdujące się w tej bazie danych – bez powtórnego analizowania wniosków certyfikacyjnych.

### 5.7.2 Postępowanie po utracie klucza prywatnego podsystemu certyfikacji

Utrata klucza prywatnego podsystemu certyfikacji, w przypadku braku podejrzeń dotyczących jego ujawnienia, powoduje następujące, niezwłocznie podejmowane działania:

- CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne (*new*with*new* oraz *old*with*new* wg RFC 4210), nową listę CRL;
- nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu CEPS 2.0, które tego wymagają, i w taki sposób aby akceptowane były również certyfikaty Subskrybentów poświadczone poprzednim,

utraconym kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły powinny traktować oba samopodpisane zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania lub, że moduły powinny traktować tylko nowe samopodpisane zaświadczenie certyfikacyjne jako punkt zaufania i posiadać dostęp do zakładkowego zaświadczenia certyfikacyjnego zawierającego dotychczasowy klucz publiczny podsystemu certyfikacji poświadczony nowym kluczem prywatnym podsystemu certyfikacji;
- CC dostarcza Subskrybentom nowe samopodpisane zaświadczenia certyfikacyjne (*new*with*new* i *old*with*new*) lub odpowiednie zakładkowe zaświadczenia certyfikacyjne w sposób zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych (o ile to możliwe w ramach protokołów dostępu do systemu CEPS 2.0, w pozostałych przypadkach w sposób uzgodniony z Subskrybentem), tj. najważniejsza jest autentyczność zaświadczenia *new*with*new*, gdyż autentyczność pozostałych jest zapewniona poprzez użycie nowego punktu zaufania.

Jeśli baza danych podsystemu certyfikacji jest wiarygodna pomimo utraty klucza, decyzją Gestora systemu nowe certyfikaty można wygenerować w oparciu o certyfikaty znajdujące się w tej bazie danych – bez powtórnego analizowania wniosków certyfikacyjnych.

## 5.8. Zakończenie działalności podsystemu certyfikacji

Decyzję o zakończeniu działalności podsystemu certyfikacji podejmuje Gestor systemu. Subskrybenci zostają poinformowani pisemnie o planowanym zakończeniu działalności podsystemu certyfikacji niezwłocznie po podjęciu takiej decyzji, w miarę możliwości z co najmniej 3-miesięcznym wyprzedzeniem. Nie później niż z chwilą zaprzestania działalności wszystkie wystawione certyfikaty zostają unieważnione.

Gdy CC zamierza przestać publikowania listy CRL, to na ostatniej liście udostępnianej w sposób, który jest określony w rozszerzeniu *CRL Distribution Point* certyfikatów, CC umieszcza w polu *nextUpdate* tej listy CRL wartość „99991231235959Z".

# 6. Zabezpieczenia techniczne

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa systemu CEPS 2.0.

W niniejszym rozdziale zawarto jedynie niektóre aspekty dotyczące zabezpieczeń technicznych.

## 6.1. Generowanie i instalowanie par kluczy

### 6.1.1 Generowanie par kluczy

Pary kluczy podsystemu certyfikacji generowane są przez personel CC zgodnie z procedurami operacyjnymi CC. Generowanie par kluczy każdego podsystemu certyfikacji odbywa się w aplikacji działającej na wydzielonym stanowisku komputerowym i w fizycznie wydzielonym, bezpiecznym pomieszczeniu. Generowanie par kluczy podsystemu CC odbywa się pod podwójną kontrolą, przez personel pełniący odpowiednie role. Po wygenerowaniu kluczy tworzony jest raport potwierdzający, że stosowna ceremonia, o której mowa powyżej, została przeprowadzona zgodnie z ustaloną procedurą oraz, że zapewniono integralność pary kluczy i poufność klucza prywatnego.

Raport dot. ceremonii generacji par kluczy musi zostać podpisany przez osoby uczestniczące w ceremonii generacji.

Pary kluczy Inspektorów ds. rejestracji generowane są przez personel CC zgodnie z procedurami operacyjnymi CC.

Generowanie par kluczy infrastruktury odbywa się w oprogramowaniu PR.

Jeśli pary kluczy Subskrybentów generowane są w PR, PR zapewnia, że:

1. Stosowane środki techniczne i organizacyjne zapewniają poufność tworzenia kluczy Subskrybenta.
2. Nie istnieje możliwość przechowywania ani kopiowania kluczy prywatnych Subskrybenta lub innych danych, które mogłyby służyć do odtworzenia klucza.
3. Nie udostępnia nikomu postronnemu kluczy prywatnych Subskrybenta, nośnik z kluczami jest wydawany tylko osobie upoważnionej przez Subskrybenta.

Jeśli pary kluczy Subskrybentów generowane są przez Subskrybenta to na niego ciąży obowiązek zapewnienia odpowiedniej jakości kluczy. Podczas generacji kluczy Subskrybent zobowiązany jest przestrzegać zapisów określających wymagania techniczne dla komponentów technicznych określone w Ustawie i towarzyszących jej aktach wykonawczych.

W przypadku generacji kluczy w aplikacji należy wziąć pod uwagę w szczególności sposób generacji ciągu losowego, natomiast w przypadku generacji kluczy, które będą przechowywane i wykorzystywane na urządzeniach typu HSM lub karta elektroniczna – bezpieczeństwo procesu

generacji jest zapewnione poprzez użycie urządzeń lub kart elektronicznych, które mają stosowny certyfikat.

### 6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

#### 6.1.2.1 Klucze generowane w PR

Klucze prywatne wraz z certyfikatami dostarczane są Subskrybentowi przez PR na nośnikach typu karta kryptograficzna. Każdej dostarczanej parze kluczy towarzyszy PIN do karty.

Wykaz nośników typu karta kryptograficzna obsługiwanych przez PR zatwierdzany jest przez Gestora systemu.

### 6.1.3 Dostarczenie klucza publicznego Subskrybenta do PR

**Tryb off-line**

W przypadku generowania pary kluczy przez Subskrybenta, klucz publiczny Subskrybenta jest dostarczany do PR w postaci pliku, zawierającego zgłoszenie certyfikacyjne w formacie PKCS#10. Zgłoszenie certyfikacyjne powinno być zgodne z profilem certyfikatów określonym w niniejszej polityce.

Na jednym nośniku może być zapisanych wiele plików ze zgłoszeniami certyfikacyjnymi.

### 6.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji

Klucze publiczne podsystemów certyfikacji są dostarczane administratorom systemu CEPS 2.0 i udostępniane Subskrybentom.

Klucze publiczne podsystemów certyfikacji są dostarczane w formie samopodpisanych zaświadczeń certyfikacyjnych, przy czym w przypadku kolejnych edycji kluczy danego podsystemu generowane są certyfikaty zakładkowe (ang. *link-certificate*).

Wszystkie nowe certyfikaty podsystemu są publikowane w Repozytorium oraz po uzgodnieniu mogą być przesyłane mail'em do Subskrybentów.

### 6.1.5 Rozmiary kluczy

Klucze urzędu certyfikacji oraz klucze urządzeń w zależności od podsystemu mają długość:

- Operatorzy CEPS 2.0 – 2048 bity

- Infrastruktura CEPS 2.0 – 2048 bity

Klucze Subskrybentów mają długość:

- Operatorzy CEPS 2.0 – 2048 bity
- Infrastruktura CEPS 2.0 – 2048 bity

W ramach niniejszej polityki certyfikacji dopuszcza się wystawianie Subskrybentom tylko certyfikatów kluczy publicznych przeznaczonych do stosowania w algorytmie RSA.

### 6.1.6 Cel użycia klucza

Treść rozszerzenia *keyUsage* oraz *extKeyUsage* w certyfikatach zgodnych z Zaleceniem X.509:2000 określa zastosowanie (jedno lub kilka) klucza publicznego zawartego w certyfikacie.

Klucz prywatny podsystemu certyfikacji może być wykorzystywany tylko do podpisywania certyfikatów, zaświadczeń certyfikacyjnych i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów, zaświadczeń certyfikacyjnych i list CRL. Samopodpisane zaświadczenia certyfikacyjne i zakładkowe zaświadczenia certyfikacyjne mają ustawione odpowiednie wartości (*cRLSign* i *keyCertSign*) w polu rozszerzenia *keyUsage*.

Klucze prywatne Inspektorów ds. rejestracji mogą być wykorzystane tylko do podpisywania zgłoszeń certyfikacyjnych i innych komunikatów przesyłanych do CC. Odpowiadające im klucze publiczne mogą być używane wyłącznie do weryfikowania zgłoszeń certyfikacyjnych i innych komunikatów przesyłanych do CC. Certyfikaty tych kluczy mają ustawione odpowiednie wartości (*nonRepudiation*) w polu rozszerzenia keyUsage.

Klucze prywatne infrastruktury mogą być używane tylko do ochrony transmisji komunikatów przesyłanych pomiędzy CC i PR. Odpowiadające im klucze publiczne mogą być używane wyłącznie do uwierzytelnienia podmiotów i szyfrowania kluczy sesyjnych podczas komunikacji pomiędzy CC i PR. Certyfikaty tych kluczy mają ustawione odpowiednie wartości (*digitalSignature* lub *keyAgreement* lub *keyEncipherment* albo wszystkie te wartości jednocześnie) w polu rozszerzenia *keyUsage*.

Klucze prywatne Subskrybentów mogą być używane tylko do podpisywania poleceń przesyłanych do systemu CEPS 2.0. Każdy z kluczy prywatnych Subskrybenta może realizować jeden lub więcej spośród tych celów. Odpowiadające im klucze publiczne mogą być używane do weryfikowania podpisu Subskrybenta lub do uwierzytelnienia Subskrybenta i szyfrowania klucza sesyjnego podczas komunikacji z systemem CEPS 2.0. Certyfikaty kluczy Subskrybenta mają ustawione odpowiednie wartości (*digitalSignature*, *keyEncipherment*, *keyAgreement* lub pewien podzbiór tych wartości) w rozszerzeniu *keyUsage*.

## 6.2. Ochrona kluczy prywatnych

### 6.2.1 Standardy dla modułów kryptograficznych

Klucze prywatne podsystemów certyfikacji generowane są w aplikacji działającej na wydzielonym stanowisku komputerowym. Zapisywane są one w postaci zaszyfrowanej do pliku typu PKCS#12 zabezpieczonego hasłem.

Klucze prywatne Inspektorów ds. rejestracji generowane są w aplikacji działającej na wydzielonym stanowisku komputerowym na imiennym koncie systemowym zabezpieczonym hasłem. Zapisywane są one w postaci zaszyfrowanej do pliku typu PKCS#12 zabezpieczonego hasłem.

Klucze prywatne infrastruktury przetwarzane są w stacjach roboczych w PR.

Klucze prywatne Subskrybentów, którzy posiadają certyfikaty imienne, mogą być przechowywane i przetwarzane wyłącznie na nośnikach kluczy kryptograficznych posiadających certyfikat[5] SSCD/QSCD.

### 6.2.2 Wieloosobowe zarządzanie kluczem

Klucze prywatne podsystemów certyfikacji nie są przechowywane z wykorzystaniem mechanizmu podziału sekretów w schemacie progowym odpowiedniego stopnia.

### 6.2.3 Powierzenie klucza prywatnego (*key-escrow)*

Udostępnienie klucza prywatnego innemu podmiotowi niż właściciel, nie występuje.

### 6.2.4 Kopia bezpieczeństwa klucza prywatnego

Kopie bezpieczeństwa kluczy prywatnych podsystemów certyfikacji są przechowywane w systemie backup-u zgodnie z zasadami określonymi w dokumentacji bezpieczeństwa systemu CEPS 2.0.

Kopie bezpieczeństwa kluczy prywatnych Subskrybenta nie są tworzone. Jeśli zasada zachowania ciągłości pracy jest dla danego Subskrybenta istotna, powinien on to przewidzieć i zapewnić rezerwowe nośniki kluczy kryptograficznych i certyfikaty, przy czym nie dotyczy to certyfikatów imiennych.

### 6.2.5 Archiwowanie klucza prywatnego

Archiwizowanie kluczy prywatnych podsystemu certyfikacji CC wynika z

[5] dopuszcza się sytuację, kiedy stosowny certyfikat na kartę kryptograficzną wygasł, ale wcześniej nie został odwołany z powodu wykrycia słabości w zabezpieczeniach

z zasad określonych w dokumentacji bezpieczeństwa systemu CEPS 2.0.

### 6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Klucze prywatne podsystemu certyfikacji są wprowadzane do aplikacji generującej certyfikaty i listy CRL przez personel CC zgodnie z procedurami operacyjnymi, przy czym instalacja i odzyskiwanie par kluczy CA w wydzielonym stanowisku komputerowym wymaga jednoczesnej kontroli co najmniej dwóch zaufanych pracowników.

W przypadku kluczy prywatnych Inspektorów ds. rejestracji wprowadzanie klucza prywatnego do modułu kryptograficznego nie występuje.

### 6.2.7 Metoda aktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji jest uaktywniany przez personel CC, zgodnie z procedurami operacyjnymi, poprzez wprowadzenie hasła chroniącego dostęp do kluczy kryptograficznych przechowywanych w pliku.

Klucze prywatne Inspektorów ds. rejestracji są aktywowane przez Inspektorów ds. rejestracji poprzez wprowadzenie na klawiaturze stacji roboczej PR haseł chroniących dostęp do zaszyfrowanych plików z kluczami kryptograficznymi.

### 6.2.8 Metoda dezaktywacji klucza prywatnego

Klucz prywatny podsystemów certyfikacji może zostać dezaktywowany przez personel CC poprzez usunięcie z aplikacji generującej certyfikaty i listy CRL oraz skasowanie pliku zawierającego parę kluczy (PKCS#12).

Dezaktywacji kluczy prywatnych Subskrybentów dokonuje się poprzez wyjęcie ich nośnika typu karta kryptograficzna z czytnika lub skasowanie pliku zawierającego parę kluczy (PKCS#12).

### 6.2.9 Metoda niszczenia klucza prywatnego

Klucze prywatne podsystemów certyfikacji niszczone są poprzez usunięcie z aplikacji generującej certyfikaty i listy CRL oraz skasowanie pliku zawierającego parę kluczy (PKCS#12). Klucze prywatne Inspektorów ds. rejestracji są niszczone poprzez skuteczne ich usunięcie z dysku komputera.

Subskrybent powinien opracować zasady, według których niszczone lub kasowane są należące do niego klucze prywatne i nośniki kluczy kryptograficznych. W przypadku, gdy nośniki kluczy kryptograficznych, na których zapisane są klucze prywatne zostały wydane przez CC i nie są własnością Subskrybenta, zasady niszczenia kluczy (i ewentualnie nośników) powinny być uzgodnione z Gestorem systemu, a każdorazowe zniszczenie nośnika zgłaszane do CC.

Klucze przechowywane na nośnikach danych powinny zostać zniszczone przez Subskrybenta lub personel CA poprzez fizyczne skasowanie (nadpisanie) danych na nośniku lub zniszczenie nośnika oraz skasowanie kluczy w urządzeniach/aplikacjach korzystających z tych kluczy.

## 6.3. Inne aspekty zarządzania parą kluczy

### 6.3.1 Długoterminowa archiwizacja kluczy publicznych i innych danych

CC prowadzi długoterminową archiwizację kluczy publicznych podsystemu certyfikacji oraz wszystkich wystawionych przez siebie certyfikatów, zaświadczeń certyfikacyjnych oraz list CRL i tokenów OCSP. Ponadto archiwizacji podlegają wszystkie dane i pliki dotyczące rejestrowanych danych o zabezpieczeniach systemu, danych o żądaniach certyfikacyjnych, informacje o Subskrybentach oraz historie kluczy, którymi posługują się urzędy certyfikacji.

Archiwizacji podlegają następujące dane:

- dane z przeglądu i oceny (z audytu) zabezpieczeń logicznych i fizycznych systemu komputerowego urzędu certyfikacji, punktu rejestracji (PR) oraz Repozytorium,
- otrzymywane wnioski, w tym postać elektroniczna i papierowa,
- baza danych certyfikatów i zaświadczeń certyfikacyjnych,
- wydane listy CRL,
- wygenerowane odpowiedzi (tokeny) OCSP,
- historia kluczy urzędu certyfikacji, od ich wygenerowania do zniszczenia włącznie.

Dostęp do archiwum mają tylko uprawnione osoby pełniące zaufane role w CC.

### 6.3.2 Okresy ważności kluczy

Okres ważności samopodpisanych zaświadczeń certyfikacyjnych podsystemów CEPS 2.0 wynosi maksymalnie 5 lat.

Okres ważności zakładkowych zaświadczeń certyfikacyjnych wynosi co najwyżej 2 lata, przy czym jest on determinowany okresem ważności wydanych przy pomocy „starego” klucza certyfikatów Subskrybentów. Koniec okresu ważności zakładkowych zaświadczeń certyfikacyjnych danego podsystemu CC jest bowiem równy końcowi okresu ważności ostatnio wygenerowanego certyfikatu Subskrybenta, podpisanego (opieczętowanego) starym kluczem danego podsystemu CC.

Okres ważności certyfikatów kluczy Inspektorów ds. rejestracji jest nie dłuższy niż 2 lata.

Okres ważności certyfikatów kluczy Subskrybentów jest nie dłuższy niż 2 lata.

## 6.4. Dane aktywujące

W CC występują następujące dane aktywujące:

1. Hasła dostępu do systemu operacyjnego.
2. Hasła dostępu do programu *Centaur CCiGK*.
3. Hasła dostępu do bazy danych CCiGK i bazy logu CCiGK.
4. Hasła dostępu do pliku z kluczami CA.

W PR występują następujące dane aktywujące:

1. Hasła dostępu do systemu operacyjnego.
2. Hasła dostępu do pliku z kluczami Inspektorów ds. rejestracji

Dane aktywujące w CC i PR są zarządzane zgodnie z procedurami umieszczonymi w odrębnych dokumentach.

U Subskrybentów występują co najmniej następujące dane aktywujące:

1) PIN'y do nośników kluczy kryptograficznych typu karta kryptograficzna lub
2) hasła dostępowe do urządzeń przetwarzających klucze prywatne Subskrybentów.

Mogą wystąpić również inne dane aktywujące. Sposób zarządzania i postępowania z danymi aktywującymi określa Subskrybent.

## 6.5. Zabezpieczenia komputerów

Szczegółowe procedury i zabezpieczenia komputerów zostały określone w dokumentach bezpieczeństwa systemu CEPS 2.0 oraz innej dokumentacji systemu.

## 6.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

### 6.6.1 Środki przedsięwzięte dla zapewnienia bezpieczeństwa rozwoju systemu

W CC przyjęto zasady dokonywania modyfikacji lub zmian w systemie teleinformatycznym. W szczególności dotyczy to testów nowych wersji oprogramowania i/lub wykorzystania do tego celu istniejących baz danych. Zasady te gwarantują nieprzerwaną pracę systemu teleinformatycznego, integralność jego zasobów oraz zachowanie poufności danych.

Integralność systemów i informacji CC jest chroniona przed wirusami, złośliwym i nieautoryzowanym oprogramowaniem.

CC określa i stosuje procedury zapewniające, że:

- łatki bezpieczeństwa (ang. *security patches*) są wdrażane w rozsądnym czasie po ich udostępnieniu;
- łaty bezpieczeństwa nie są wdrażane, jeśli wprowadzają dodatkowe podatności lub niestabilności, które przewyższają korzyści wynikające z ich zastosowania; oraz

- powody niestosowania łatek bezpieczeństwa są dokumentowane.

### 6.6.2 Zarządzanie bezpieczeństwem

Za realizację procesów bezpieczeństwa jest odpowiedzialny personel CC. Środki bezpieczeństwa zostały określone w dokumentacji bezpieczeństwa systemu CEPS 2.0.

## 6.7. Zabezpieczenia sieci komputerowej

Nie przewiduje się podłączenia żadnego z podsystemów CC do rozległej sieci komputerowej (WAN) w zakresie operacji wymagających użycia odpowiedniego klucza prywatnego, przy czym stosowne repozytoria udostępniające zaświadczenia certyfikacyjne i listy CRL są dostępne on-line, ale w ramach wydzielonej sieci komputerowej niedostępnej publicznie.

Szczegółowe procedury i zabezpieczenia sieci komputerowej zostały określone w dokumentacji bezpieczeństwa systemu CEPS 2.0.

## 6.8. Oznaczanie czasem

Do oznaczania czasem certyfikatów, zaświadczeń certyfikacyjnych, list CRL oraz zapisów w logach urządzeń i oprogramowania stosuje się wskazanie bieżącego czasu pochodzące z zegara synchronizowanego z czasem UTC przynajmniej raz dziennie.

Zakres niniejszego dokumentu nie obejmuje polityki wystawiania znaczników czasu.

# 7. Profil certyfikatów i list CRL

Rozdział zawiera informacje o profilu certyfikatów kluczy publicznych i list CRL generowanych zgodnie z niniejsza polityką certyfikacji.

## 7.1. Profil certyfikatów

CC wystawia certyfikaty i zaświadczenia certyfikacyjne w formacie zgodnym z Zaleceniem X.509:2000, wersja 3 formatu.

Zaświadczenia certyfikacyjne i certyfikaty zawierają następujące pola:

| Pole | Opis/wartość |
|---|---|
| tbsCertificate | Poświadczona elektronicznie treść certyfikatu, opisana jest szczegółowo w rozdziale 7.1.1 i 7.1.2. |
| signatureAlgorithm | Identyfikator algorytmu służącego do opieczętowania zaświadczenia certyfikacyjnego/certyfikatu |
| Algorithm | Jeden z poniższych OID'ów:<br>{1.2.840.113549.1.1.11} (sha256WithRSAEncryption)<br>{1.2.840.113549.1.1.13} (sha512WithRSAEncryption) |
| parameters | Null |
| signatureValue | Wartość poświadczenia elektronicznego (pieczęci elektronicznej) |

### 7.1.1 Pola podstawowe

#### 7.1.1.1 Zaświadczenia certyfikacyjne

Pola podstawowe zaświadczeń certyfikacyjnych (ang. *CA certificate*) mają strukturę, przedstawioną w poniższej tabeli:

| Pole | Wartość | Uwagi |
|---|---|---|
| *version* | 2 | Zgodny z zaleceniem X.509:2000, wersja 3 formatu |
| *serialNumber* | | Jednoznaczny w ramach centrum wydającego certyfikat |
| *signature* | | Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu łącznie ze wskazaniem funkcji skrótu; wartość identyczna, jak w polu *Algorithm* (rozdz. 7.1) |
| *issuer* | C = PL<br>O = Minister właściwy ds informatyzacji<br>OU = CEPS<br>CN = Operatorzy lub Infrastruktura | Nazwa wyróżniająca CA w systemie produkcyjnym |

| Pole | Wartość | Uwagi |
|---|---|---|
| | C = PL<br>O = Minister właściwy ds informatyzacji<br>OU = CEPS-TEST<br>CN = Operatorzy lub Infrastruktura | Nazwa wyróżniająca CA w systemie testowym |
| *validity* | | |
| *not before* | | Data i godzina wydania certyfikatu |
| *not after* | | Data i godzina wydania certyfikatu + *<okres ważności certyfikatu>* (5 lat w przypadku *self-signed* certyfikatów; najstarszy okres ważności EE certyfikatu podpisanego „starym" kluczem CA w przypadku *link-certificate: old*with*new* i *new*with*old*) |
| *subject* | Jak w polu *issuer* | Zaświadczenia certyfikacyjne są typu *self-issued* |
| *subjectPublicKeyInfo* | | |
| *algorithm* | OID: 1.2.840.113549.1.1.1<br>(*rsaEncryption*) | Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu |
| *subjectPublicKey* | | Klucz publiczny posiadacza certyfikatu |

### 7.1.1.2 EE certyfikaty

Pola podstawowe EE certyfikatów (ang. *End Entity Certificate*) mają strukturę, przedstawioną w poniższej tabeli:

| Pole | Wartość | Uwagi |
|---|---|---|
| *version* | 2 | Zgodny z zaleceniem X.509:2000, wersja 3 formatu |
| *serialNumber* | | Jednoznaczny w ramach centrum wydającego certyfikat |
| *signature* | | Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu łącznie ze wskazaniem funkcji skrótu;<br>wartość identyczna, jak w polu *Algorithm* (rozdz. 7.1) |
| *issuer* | C = PL<br>O = Minister właściwy ds informatyzacji<br>OU = CEPS ( *podsystem* "*produkcyjny*") lub<br>OU = CEPS-TEST (*podsystem* "*testowy*")<br>CN = Infrastruktura | Nazwa wyróżniająca CA w podsystemie „Infrastruktura CEPS 2.0" |
| | C = PL<br>O = Minister właściwy ds informatyzacji<br>OU = CEPS ( *podsystem "produkcyjny*") lub<br>OU = CEPS-TEST ( *podsystem "testowy")*<br>CN = Operatorzy | Nazwa wyróżniająca CA w podsystemie „Operatorzy CEPS 2.0" |
| *validity* | | |
| *not before* | | Data i godzina wydania certyfikatu |

| Pole | Wartość | Uwagi |
|---|---|---|
| *not after* | | Data i godzina wydania certyfikatu + <*okres ważności certyfikatu*> (max. 2 lata) |
| *subject* | Patrz rozdz. 3.1.1 | Nazwa wyróżniająca Subskrybenta w podsystemie „Infrastruktura CEPS 2.0” |
| | C = PL<br>O= Minister właściwy ds informatyzacji<br>OU = CEPS ( *podsystem* “*produkcyjny*”) lub<br>OU = CEPS-TEST (podsystem “testowy”)<br>CN = OCSP Infrastruktura | Nazwa wyróżniająca serwera OCSP w podsystemie „Infrastruktura CEPS 2.0” |
| | Patrz rozdz. 3.1.2 | Nazwa wyróżniająca Subskrybenta w podsystemie „Operatorzy CEPS 2.0” |
| | C = PL<br>O = Minister właściwy ds informatyzacji<br>OU = CEPS( *podsystem* “*produkcyjny*”) lub<br>OU = CEPS-TEST (podsystem “testowy”)<br>CN = OCSP Operatorzy | Nazwa wyróżniająca serwera OCSP w podsystemie „Operatorzy CEPS 2.0” |
| *subjectPublicKeyInfo* | | |
| *algorithm* | OID: 1.2.840.113549.1.1.1<br>(*rsaEncryption*) | Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu |
| *subjectPublicKey* | | Klucz publiczny posiadacza certyfikatu |

## 7.1.2 Rozszerzenia certyfikatów i ich krytyczność

### 7.1.2.1 Rozszerzenia zaświadczeń certyfikacyjnych

| Rozszerzenie | Opis/wartość | Krytyczne ? |
|---|---|---|
| authorityKeyIdentifier | skrót SHA1 z klucza publicznego wystawcy w polu *keyIdentifier* | NIE |
| subjectKeyIdentifier | skrót SHA1 z klucza publicznego Subskrybenta w polu *keyIdentifier* | NIE |
| keyUsage | *CRLSign*, *keyCertSign* | TAK |
| certificatePolicies | | NIE |
| policyIdentifier | OID: 0.4.0.2042.1.3<br>(identyfikator niniejszej polityki certyfikacji) | |
| basicConstraints | informacja o tym, czy Subskrybent jest urzędem certyfikacji | TAK |
| cA | TRUE | |
| cRLDistributionPoint | Adres(y), pod którym(i) będą publikowane listy CRL | NIE |

### 7.1.2.2 Rozszerzenia EE certyfikatów

#### 7.1.2.2.1 Podsystem „Infrastruktura CEPS”

| Rozszerzenie | Opis/wartość | Krytyczne ? |
|---|---|---|
| authorityKeyIdentifier | skrót SHA1 z klucza publicznego wystawcy w polu *keyIdentifier* | NIE |
| subjectKeyIdentifier | skrót SHA1 z klucza publicznego Subskrybenta w polu *keyIdentifier* | NIE |

| | | |
|---|---|---|
| keyUsage | certyfikaty służące do ochrony poufności transmisji danych (ustanowienia kluczy sesyjnych i uwierzytelnienie sesji IKE) powinny mieć ustawione bity:<br>*digitalSignature*, *keyEncipherment*, *keyAgreement* | TAK |
| | certyfikat do realizacji usługi OCSP powinien mieć ustawiony tylko bit *digitalSignature* | TAK |
| extKeyUsage | OID: 1.3.6.1.5.5.7.3.1<br>(serverAuth); dot. EE certyfikatu serwera do uwierzytelnienia sesji SSL (TLS) | NIE |
| | OID: 1.3.6.1.5.5.7.3.9<br>(OCSPSigning); dot. certyfikatu do realizacji usługi OCSP | TAK |
| certificatePolicies | | NIE |
| policyIdentifier | OID: 0.4.0.2042.1.3<br>(identyfikator niniejszej polityki certyfikacji) | |
| basicConstraints | | TAK |
| cA | pusta sekwencja<br>(określenie, że Subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów) | |
| cRLDistributionPoint | Adres(y), pod którym(i) będą publikowane listy CRL | NIE |
| authorityInfoAccess | | NIE |
| accessMethod | OID: 1.3.6.1.5.5.7.48.2<br>(caIssuers) | |
| accessLocation | adres Repozytorium, skąd można pobrać dodatkowe informacje dot. budowy ścieżek certyfikacji, np. link-certyfikaty | |
| accessMethod | OID: 1.3.6.1.5.5.7.48.1<br>(oscp)<br>Uwaga: nie dotyczy EE certyfikatu respondera OCSP | |
| accessLocation | adres serwera usługi OCSP | |

#### 7.1.2.2.2 Podsystem „Operatorzy CEPS”

| Rozszerzenie | Opis/wartość | Krytyczne ? |
|---|---|---|
| authorityKeyIdentifier | skrót SHA1 z klucza publicznego wystawcy w polu *keyIdentifier* | NIE |
| subjectKeyIdentifier | skrót SHA1 z klucza publicznego Subskrybenta w polu *keyIdentifier* | NIE |
| keyUsage | certyfikaty służące do uwierzytelnienia sesji SSL (TLS) powinny mieć ustawione bity: *digitalSignature*, *keyEncipherment*, *keyAgreement* | TAK |
| | certyfikat do realizacji usługi OCSP powinien mieć ustawiony tylko bit *digitalSignature* | TAK |
| extKeyUsage | OID: 1.3.6.1.5.5.7.3.2<br>(clientAuth); dot. EE certyfikatu klienta do uwierzytelnienia sesji SSL (TLS) | NIE |
| | OID: 1.3.6.1.5.5.7.3.9<br>(OCSPSigning); dot. certyfikatu do realizacji usługi OCSP | TAK |
| certificatePolicies | | NIE |
| policyIdentifier | OID: 0.4.0.2042.1.3<br>(identyfikator niniejszej polityki certyfikacji) | |
| basicConstraints | | TAK |
| cA | pusta sekwencja<br>(określenie, że Subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów) | |

| | | |
|---|---|---|
| cRLDistributionPoint | Adres(y), pod którym(i) będą publikowane listy CRL | NIE |
| authorityInfoAccess | | NIE |
| accessMethod | OID: 1.3.6.1.5.5.7.48.2<br>(calssuers) | |
| accessLocation | adres Repozytorium, skąd można pobrać dodatkowe informacje dot. budowy ścieżek certyfikacji, np. link-certyfikaty | |
| accessMethod | OID: 1.3.6.1.5.5.7.48.1<br>(oscp)<br>Uwaga: nie dotyczy EE certyfikatu respondera OCSP | |
| accessLocation | adres serwera usługi OCSP | |

### 7.1.3 Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów

Formaty nazw wyróżniających urzędów CA w poszczególnych podsystemach CC są określone w rozdz. 7.1.1 – pole *issuer*.

Formaty nazw wyróżniających Subskrybentów w poszczególnych podsystemach CC są określone w rozdz. 3.1.

### 7.1.4 Identyfikatory zgodnych polityk certyfikacji

OID: 0.4.0.2042.1.3

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) lcp (3)

## 7.2. Profil list CRL

CC wystawia listy CRL w formacie zgodnym z Zaleceniem X.509:2000, wersja 2 formatu.

### 7.2.1 Pola podstawowe listy CRL

| Pole | Wartość | Uwagi |
|---|---|---|
| *version* | 1 | Zgodny z zaleceniem X.509:2000, wersja 2 formatu |
| *signature* | { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }<br>(*sha256WithRSAEncryption*) | Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu łącznie ze wskazaniem funkcji skrótu |
| *issuer* | C = PL<br>O = Minister właściwy ds informatyzacji<br>OU = CEPS ( *podsystem* "*produkcyjny*") lub<br>OU = CEPS-TEST (*podsystem* "*testowy*")<br>CN = Infrastruktura | Nazwa wyróżniająca CA w podsystemie „Infrastruktura CEPS 2.0" |
| | C = PL<br>O = Minister właściwy ds informatyzacji<br>OU = CEPS ( *podsystem* "*produkcyjny*") lub<br>OU = CEPS-TEST (podsystem "testowy")<br>CN = Operatorzy | Nazwa wyróżniająca CA w podsystemie „Operatorzy CEPS 2.0" |

| Pole | Wartość | Uwagi |
|---|---|---|
| *thisUpdate* | | Data i godzina wydania listy |
| *nextUpdate* | | Data i godzina wydania listy + *<okres ważności listy>* (48 godzin) |
| *revokedCertificates* | lista numerów seryjnych odwołanych certyfikatów | |
| *serialNumber* | | Numer seryjny unieważnionego certyfikatu |
| *revocationDate* | | Data unieważnienia certyfikatu |

### 7.2.2 Rozszerzenia list CRL i wpisów na listach CRL oraz krytyczność rozszerzeń

Rozszerzenia dotyczące całej listy CRL:

| Pole | Opis/wartość | Krytyczne ? |
|---|---|---|
| crlExtensions | rozszerzenia listy CRL (dotyczą całej listy) | |
| authorityKeyIdentifier | skrót SHA1 z klucza publicznego w polu *keyIdentifier* | NIE |
| cRLNumber | numer kolejny listy CRL wystawionej w ramach podsystemu certyfikacji | NIE |

Rozszerzenia dotyczące poszczególnych unieważnionych certyfikatów lub zaświadczeń:

| Pole | Opis/wartość | Krytyczne ? |
|---|---|---|
| crlEntryExtensions | rozszerzenia listy CRL (dotyczą każdego z certyfikatów lub zaświadczeń certyfikacyjnych z osobna) | |
| cRLReason | kod przyczyny unieważnienia (**opcjonalne**) | NIE |

## 7.3. Profil OCSP

### 7.3.1 Numer wersji

W każdym podsystemie Centrum Certyfikacji świadczy usługę weryfikacji statusu certyfikatu w oparciu o protokół OCSP (ang. *Online Certificate Status Protocol*) zgodnie z RFC 6960. Zapytania OCSP (*OCSPRequest*) zawierają tylko wskazanie numeru wersji (v1) oraz identyfikator (lub identfikatory) certyfikatu(ów), o którego(ych) status jest zapytanie (*requestList*). Mogą również zawierać opcjonalne pole *requestorName*, czyli ewentualnie nazwę wysyłającego zapytanie OCSP. Odpowiedzi usługi OCSP generowane przez serwer OCSP mają postać *basic OCSP responder* (OID: 1.3.6.1.5.5.7.48.1), czyli zawierają status przesłanego zapytania (np. *successful*) oraz właściwą odpowiedź *responseBytes*[6], podpisaną (opieczętowaną) przez serwer OCSP.

### 7.3.2 Rozszerzenia OCSP

Zapytanie i odpowiedź serwera OCSP może posiadać niekrytyczne rozszerzenie *nonce*, które zawiera frazę wiążącą zapytanie z odpowiedzią. Wartość w odpowiedzi OCSP jest identyczna

[6] gdy status jest związany z błędem, pole *responseBytes* nie jest odsyłane

z frazą z zapytania. Celem zastosowania frazy jest zapobieganie atakom powtórzeniowym na serwer OCSP.

Zapytanie i odpowiedź serwera OCSP nie zawierają innych rozszerzeń.

# 8. Audyt

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

Zewnętrzny podmiot oceniający ma status „akredytowany” w rozumieniu ustawy o systemie oceny zgodności, czyli posiada certyfikat wydany przez Polskie Centrum Akredytacji (PCA) lub audyt jest wykonywany przez osoby z zewnątrz, które mają certyfikaty potwierdzające autoryzację do wykonywania audytów na zgodność z normą ISO/IEC 27001 („certyfikowani audytorzy”).

Zewnętrzny audyt odbywa się nie rzadziej niż raz na 2 lata, przy czym podmiot audytujący/certyfikowani audytorzy mogą dodatkowo narzucić dodatkowe wymagania co do audytu w ramach nadzoru, i np. rekomendują coroczny audyt częściowy w ramach nadzoru, który dotyczyłby wdrożonych poprawek dostosowawczych.

# 9. Inne postanowienia

## 9.1. Poufność informacji

Rodzaje informacji podlegające ochronie oraz sposoby ich ochrony są zdefiniowane w dokumentacji bezpieczeństwa opracowanych dla CC.

Subskrybenci są zobowiązani do ochrony poufności posiadanych kluczy kryptograficznych oraz innych danych z tym związanych (jak kody PIN). Wytyczne do zastosowania określonego poziomu ochrony materiałów kryptograficznych, w tym ewentualną klauzulę tajności zgodnie z ustawą o ochronie informacji niejawnych, nadaje Gestor systemu.

Certyfikaty, zaświadczenia certyfikacyjne i listy CRL są traktowane jako informacje jawne, o ograniczonym dostępie. Dostęp do aktualnych certyfikatów, zaświadczeń certyfikacyjnych oraz list CRL ma personel obsługujący system CEPS 2.0.

Dostęp do wystawionych im certyfikatów, zaświadczeń certyfikacyjnych oraz list CRL mogą mieć również Subskrybenci.

Zasady zachowania poufności innych informacji oraz zasady odpowiedzialności za naruszenie poufności informacji określone są w umowie podpisywanej przez Subskrybenta z MC.

## 9.2. Ochrona danych osobowych

W ramach systemu CEPS 2.0 ustanowiona jest polityka ochrony danych osobowych oraz wprowadzone mechanizmy ochrony danych osobowych zgodne z obowiązującymi przepisami.

## 9.3. Zabezpieczenie własności intelektualnej

Niniejsza polityka certyfikacji stanowi własność intelektualną MC. Z punktu widzenia prawa autorskiego polityka może być bez żadnych ograniczeń wykorzystywana (w tym drukowana i kopiowana) przez osoby, w tym Subskrybentów, którym została udostępniona za zgodą MC.

Certyfikaty wystawione przez CC są jego własnością. Subskrybenci mają prawo do wykorzystywania certyfikatów w systemie CEPS 2.0, zgodnie z zasadami opisanymi w niniejszej polityce certyfikacji.

## 9.4. Udzielane gwarancje

Nie występują.

## 9.5. Zwolnienia z domyślnie udzielanych gwarancji

Nie występują.

## 9.6. Ograniczenia odpowiedzialności

Ograniczenia odpowiedzialności są określane w umowach lub porozumieniach zawieranych pomiędzy Subskrybentami i MC.

## 9.7. Przenoszenie roszczeń odszkodowawczych

Nie występuje.

## 9.8. Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Przepisy przejściowe nie występują.

Niniejsza polityka certyfikacji obowiązuje w stosunku do certyfikatów wystawionych zgodnie z nią do utraty ważności tych certyfikatów (z powodu zakończenia okresu ważności lub unieważnienia).

W stosunku do nowo wystawianych certyfikatów stosuje się najnowszą obowiązującą politykę certyfikacji zatwierdzoną przez Gestora systemu.

## 9.9. Określanie trybu i adresów doręczania pism

Tryb i adres doręczania pism związanych ze sprawami niniejszej polityki certyfikacji i wystawianych w jej ramach certyfikatów określa umowa lub porozumienie pomiędzy Subskrybentem i MC.

## 9.10. Zmiany w polityce certyfikacji

Zasady zarządzania polityką certyfikacji zostały opisane w rozdziale 1.5.

## 9.11. Rozstrzyganie sporów

Wszelkie spory dotyczące spraw związanych z niniejszą polityką certyfikacji będą rozstrzygane przez Gestora systemu.

Wiążące interpretacje postanowień niniejszej polityki certyfikacji wydaje Gestor systemu.

## 9.12. Obowiązujące prawo

Działanie podsystemu certyfikacji podlega prawu polskiemu.

## 9.13. Podstawy prawne

Zasady działania CC są zgodne z obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:

- ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2019 r., poz. 1781);
- ustawie z dnia 6 czerwca 1997 r. Kodeks karny (tekst jednolity Dz. U. 2022, poz. 1138 ze zm.);
- ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity Dz. U. 2021, poz. 1062 ze zm.);
- ustawie z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity Dz. U. 2022, poz. 1510 ze zm.);
- ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tekst jednolity Dz. U. 2023, poz. 756 ze zm.);
- rozporządzeniu Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (D. U. 2020, poz. 399).

## 9.14. Inne postanowienia

Nie występują.