*Załącznik nr 12, część B*
*do Regulaminu świadczenia usług certyfikacyjnych*
*przez Centrum Certyfikacji Województwa Podlaskiego*

**Polityka Certyfikacji esigCA**

## 1 Wstęp

Polityka Certyfikacji esigCA Centrum Certyfikacji Województwa Podlaskiego (CCWP) prowadzonego przez Urząd Marszałkowski Województwa Podlaskiego określa ogólne zasady stosowane przez CCWP w ramach świadczonych usług certyfikacji kluczy publicznych w celu budowy zaufania użytkowników, definiuje obowiązki i odpowiedzialność uczestników Infrastruktury Klucza Publicznego, typy certyfikatów i ich obszary zastosowań.

### 1.1 Identyfikacja Polityki

| | |
|---|---|
| Nazwa polityki | Polityka Certyfikacji dla esigCA |
| Wersja | 1.0 |
| Zastrzeżenie | Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji esigCA" nie jest certyfikatem kwalifikowanym w rozumieniu ustawy z dn. 18.09.2001 o podpisie elektronicznym. |
| Status | finalna |
| Identyfikator polityki (OID) | 1.2.616.1.113637.1.2.1 |
| Data wydania | 2007-08-10 |
| Data ważności | do odwołania |

### 1.2 Historia zmian

| *Wersja* | *Data* | *Opis zmian* |
|---|---|---|
| 1.0 | 2007-08-10 | pierwsza wersja |

Kolejne wprowadzane zmiany w polityce certyfikacji – o ile nie podano inaczej - mają także zastosowanie do certyfikatów wystawionych na podstawie niniejszej polityki.

## 2 Postanowienia Polityki Certyfikacji

### 2.1 Zakres stosowalności

Odbiorcami usług certyfikacyjnych świadczonych przez CCWP są osoby fizyczne, mieszkańcy województwa Podlaskiego. Wydawane certyfikaty mają okres ważności 1 (jeden) rok.

Certyfikaty wydane zgodnie z Polityką są przeznaczone do uwierzytelnia subskrybenta w elektronicznej komunikacji z urzędami. Polityka nie wyklucza wykorzystania wydanych certyfikatów do uwierzytelniania względem zewnętrznych instytucji.

Certyfikaty wydawane w ramach Polityki nie są certyfikatami kwalifikowanymi w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450). W szczególności podpis elektroniczny weryfikowany na podstawie certyfikatu nie jest równorzędny w skutkach z podpisem własnoręcznym.

## 2.2 Prawa i obowiązki

### 2.2.1 Obowiązki Subskrybenta

Przed uzyskaniem certyfikatu, wnioskodawca zobowiązany jest do zapoznania się z treścią Polityki. Złożenie wniosku o wydanie certyfikatu jest równoznaczne z akceptacją warunków świadczenia usługi.

Osoba będąca Subskrybentem zobowiązana jest do bezpiecznego przechowywania swojego klucza prywatnego, karty mikroprocesorowej, oraz ochrony kodu PIN karty w sposób zapobiegający jego ujawnieniu.
W przypadku utraty kontroli nad kluczem prywatnym, odpowiadającym kluczowi publicznemu umieszczonemu w certyfikacie, ujawnieniu kodu PIN lub też uzasadnionego podejrzenia, iż fakty takie mogły mieć miejsce, Subskrybenta zobowiązuje się do niezwłocznego powiadomienia o tym fakcie wydawcę certyfikatu poprzez złożenie wniosku o unieważnienie certyfikatu.

Subskrybent jest odpowiedzialny za prawdziwość danych przekazywanych we wniosku o wydanie certyfikatu.
Subskrybent certyfikatu zobowiązuje się do informowania wydawcy certyfikatu o wszelkich zmianach informacji zawartych we wniosku o wydanie certyfikatu.

Po upływie daty ważności Subskrybent ma obowiązek zaprzestać używania klucza prywatnego (karty mikroprocesorowej) skojarzonego z kluczem publicznym zawartym w tym certyfikacie i zwrócić kartę mikroprocesorową co CCWP w przeciągu 14 dni.

### 2.2.2 Obowiązki strony ufającej

Strona ufająca jest zobowiązana do pobrania z Repozytorium w sposób bezpieczny certyfikatu pośredniego Centrum Certyfikacji Województwa Podlaskiego, który otrzymała oraz zweryfikowania skrótu klucza publicznego CCWP.

W trakcie określania swojego zaufania wobec usługi bazującej na certyfikacie wydanym w ramach Polityki, obowiązkiem Subskrybenta jest przeprowadzenie stosownej weryfikacji ważności certyfikatu. W procesie weryfikacji Subskrybenta strona ufająca musi zweryfikować ścieżkę certyfikacji przy użyciu informacji publikowanych przez CCWP w Repozytorium.

### 2.2.3 Obowiązki CCWP

CCWP odpowiada za weryfikację danych zamieszczonych we wniosku o wydanie certyfikatu z danymi zawartymi w dokumentach wnioskodawcy oraz za publikowanie informacji o unieważnieniach certyfikatów zgodnie z procedurami opisanymi w Regulaminie.

## 2.3 Publikacja i repozytorium

CCWP nie publikuje certyfikatów subskrybentów wydanych w ramach Polityki. Informacja o unieważnionych certyfikatach jest publikowana w Repozytorium w chwili tworzenia nowej listy certyfikatów unieważnionych. Nowa lista certyfikatów unieważnionych dla certyfikatów wydawanych zgodnie z Polityką jest tworzona w terminie do 1 godziny po każdym unieważnieniu certyfikatu, jednak nie rzadziej, niż co 7 dni.

## 2.4 Ochrona informacji

Dane osobowe przechowywane i przetwarzane w ramach realizacji Polityki podlegają ochronie zgodnie z ustawą o ochronie danych osobowych oraz powszechnie obowiązującymi przepisami prawa. Centrum gwarantuje, że informacje nie będą udostępniane osobom postronnym.

## 3 Identyfikacja i uwierzytelnienie

### 3.1 Rejestracja

Procedurę złożenie wniosku o wydanie certyfikatu określa Regulamin.

Wnioskodawca powinien dostarczyć wniosek zawierający następujące dane :

- imię i nazwisko
- organizację i jednostkę organizacyjną wnioskodawcy – jeżeli występuje
- adres zamieszkania (zameldowania)
- numer PESEL
- adres poczty elektronicznej
- numer telefonu kontaktowego

Wniosek o wydanie certyfikatu należy składać w Punkcie Rejestracji w Urzędzie Marszałkowskim Województwa Podlaskiego w Białymstoku, ul. Kard. Stefana Wyszyńskiego 1.

Weryfikacja danych zawartych we wniosku przeprowadzania jest przez pracownika Punktu Rejestracji na podstawie danych zawartych w dokumencie tożsamości.

Wydanie certyfikatu jest możliwe w Punkcie Rejestracji, w którym złożony został wniosek. Od momentu wydania wnioskodawca staje się Subskrybentem - posiadaczem karty elektronicznej (nośnika klucza prywatnego i certyfikatu) i odpowiada za jej bezpieczeństwo. Termin wydania certyfikatu określa Regulamin.

### 3.2 Odnowienie certyfikatu

Certyfikat wydany zgodnie z Polityką może być odnowiony. Odnawianie certyfikatu jest równoznaczne z wydaniem nowego certyfikatu zawierającego jednakowe, z wyjątkiem okresu ważności i klucza publicznego, dane. Centrum Certyfikacji nie wydaje nowego certyfikatu dla klucza publicznego zawartego w certyfikacie.

Odnowienie certyfikatu może nastąpić po upływie terminu ważności odnawianego certyfikatu.
Podczas odnowienia certyfikatu jest sprawdzany dostęp Subskrybenta do klucza prywatnego. Tożsamość Subskrybenta certyfikatu nie jest weryfikowana.

Celem odnowienia certyfikatu Subskrybent musi dostarczyć kartę mikroprocesorową do Punktu Rejestracji wraz z wnioskiem o odnowienie certyfikatu.

### 3.3 Akceptacja certyfikatu

Właściciel certyfikatu zobowiązany jest do zweryfikowania poprawności danych zawartych w certyfikacie z danymi zawartymi we wniosku. W przypadku stwierdzenia niezgodności zobowiązany jest do niezwłocznego zawiadomienia CCWP o tym fakcie i złożenia wniosku o unieważnienie certyfikatu. CCWP zobowiązany jest do wydania nowego poprawionego certyfikatu. Brak zgłoszenia o niezgodności w ciągu 24 godzin jest równoważne z potwierdzeniem zgodności danych.

Akceptacja certyfikatu zawierającego niepoprawne dane przez Subskrybenta obciąża go skutkami prawnymi używania tego certyfikatu.

### 3.4 Unieważnienie certyfikatu

Do unieważnienia certyfikatu wystawionego zgodnie z niniejszą Polityką Certyfikacji wymagane jest przesłanie odpowiedniego wniosku o unieważnienie i weryfikacja uprawnień do złożenia takiego wniosku.

Warunkiem rozpoczęcia procedury unieważnienia certyfikatu jest złożenie przez właściciela lub uprawnioną stronę trzecią wniosku o wykonanie tej czynności. Tożsamość wnioskodawcy weryfikuje się na podstawie ważnego dowodu

tożsamości.

Certyfikat jest również unieważniany w następujących przypadkach:

1. otrzymania pisemnego wniosku o unieważnieni certyfikatu od uprawnionej osoby trzeciej;
2. zdezaktualizowania informacji zawartych w certyfikacie;
3. niedozwolonego lub błędnego wydanie certyfikatu na skutek:
   - fałszerstwa danych zawartych w certyfikacie,
   - niespełnienia istotnych warunków wstępnych do wydania certyfikatu,
   - popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania.

Unieważnienie certyfikatu jest procedurą NIEODWRACALNĄ.

## 4 Techniczne środki zapewnienia bezpieczeństwa

### 4.1 Generowanie pary kluczy

Polityka wymaga aby para kluczy subskrybenta była wygenerowana zgodnie z algorytmem RSA. Długość klucza (rozumiana jako moduł p*q) – co najmniej 1024 bitów.

Generowanie pary kluczy będzie wykonywane przez pracownika Centrum Certyfikacji, w bezpiecznym urządzeniu – karcie kryptograficznej. W momencie generowania pary kluczy jest nadawany kod PIN przypisany do karty kryptograficznej. Karta pozostaje w Punkcie Rejestracji do momentu nadania Certyfikatu i wgrania go na kartę mikroprocesorową.

### 4.2 Ochrona klucza prywatnego subskrybenta

Za ochronę klucza prywatnego (karty mikroprocesorowej) skojarzonego z kluczem publicznym umieszczonym w certyfikacie odpowiedzialny jest wyłącznie Subskrybent.

### 4.3 Niszczenie kluczy

Karta mikroprocesorowa, zawierająca klucz prywatny, skojarzony z kluczem publicznym z certyfikatu, którego ważność wygasła powinna zostać zwrócona do Punktu Rejestracji celem zniszczenia tego klucza.

## 5 Możliwość dostosowania Polityki do wymagań subskrybenta

Subskrybent nie ma możliwości zmiany Polityki.