Załącznik nr 12. część D
do Regulaminu świadczenia usług certyfikacyjnych
przez Centrum Certyfikacji Województwa Podlaskiego

Polityka Certyfikacji netCA

1 Wstęp

Polityka Certyfikacji netCA 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 netCA
Wersja	1.0
Zastrzeżenie	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji netCA" nie jest certyfikatem kwalifikowanym w rozumieniu ustawy z dn. 18.09.2001 o podpisie elektronicznym.
Status	Finalna
Identyfikator polityki (OID)	1.2.616.1.113637.1.4.1
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

Certyfikaty wydane zgodnie z Polityką są przeznaczone do zabezpieczenia komunikacji sieciowej. W szczególności posiadaczem certyfikatu może być administrator lub właściciel urządzenia sieciowego.

Wydawane certyfikaty są przeznaczone do:
- zestawiania połączeń w wirtualnych sieciach prywatnych.
- uwierzytelnienia serwerów sieciowych oraz zestawienia bezpiecznego połączenia w protokole SSL.
- innych celów precyzowanych umową między subskrybentem a Centrum Certyfikacji

Certyfikaty wydane zgodnie z Polityką są wydawane na wniosek osoby odpowiedzialnej za działanie urządzenia sieciowego nie są potwierdzeniem posiadania praw do dysponowania adresem IP lub nazwą domenową zawartą w certyfikacie. Wydawane certyfikaty mają okres ważności 1 (jeden) rok.

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), i nie służą do weryfikacji podpisu elektronicznego.

2.2 Prawa i obowiązki

2.2.1 Obowiązki posiadacza certyfikatu

Przed uzyskaniem certyfikatu, wnioskodawca zobowiązany jest do zapoznania się z treścią Polityki. Złożenie wniosku o wydanie certyfikatu jest równoznaczne z akceptacją warunków świadczenia usługi.
Strona będąca posiadaczem certyfikatu zobowiązana jest do bezpiecznego przechowywania swojego klucza prywatnego.
W przypadku utraty kontroli nad kluczem prywatnym, odpowiadającym kluczowi publicznemu umieszczonemu w certyfikacie, jego ujawnieniu lub też uzasadnionego podejrzenia, iż fakt taki mógł mieć miejsce, posiadacz certyfikatu zobowiązuje się niezwłocznie powiadomić o tym wydawcę certyfikatu poprzez złożenie wniosku o unieważnienie tego certyfikatu.

Posiadacz certyfikatu jest odpowiedzialny za prawdziwość danych zawartych we wniosku o wydanie certyfikatu.
Posiadacz certyfikatu zobowiązuje się do informowania wydawcy certyfikatu o wszelkich zmianach informacji zawartych w jego certyfikacie lub podanych we wniosku o wydanie certyfikatu.

2.2.2 Obowiązki strony ufającej

Strona ufająca jest zobowiązana do pobrania w sposób bezpieczny certyfikatu CCWP, który obdarzyła zaufaniem oraz zweryfikowania skrótu klucza publicznego CCWP.
W trakcie określania swojego zaufania wobec usługi bazującej na certyfikacie wydanym w ramach Polityki, obowiązkiem strony ufającej jest przeprowadzenie stosownej weryfikacji ważności certyfikatu. W procesie weryfikacji strona ufająca musi zweryfikować ścieżkę certyfikacji przy użyciu informacji publikowanych przez CCWP w Repozytorium.

2.2.3 Obowiązki CCWP

CCWP odpowiada za weryfikację i zgodność informacji zawartych w wydanych certyfikatach z danymi zamieszczonymi we wniosku oraz odpowiada za publikowanie informacji o unieważnionych certyfikatach zgodnie z procedurami opisanymi w niniejszym dokumencie. CCWP nie odpowiada za prawdziwość tych danych.

2.3 Publikacja i repozytorium

Informacja o unieważnieniu certyfikatu jest publikowana 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. Lista certyfikatów unieważnionych jest publikowana w Repozytorium.

2.4 Ochrona informacji

Dane przechowywane i przetwarzane w ramach realizacji Polityki podlegają ochronie obowiązującymi przepisami prawa. Centrum gwarantuje, że stronie ufającej udostępniane są wyłącznie informacje zawarte w certyfikacie.

2.5 Interpretacja i obowiązujące akty prawne

Funkcjonowanie Centrum Certyfikacji oparte jest na zasadach ujętych w Regulaminie.

3 Identyfikacja i uwierzytelnienie

3.1 Rejestracja

Wydanie certyfikatu musi być poprzedzone złożeniem odpowiedniego wniosku w CCWP. Do centrum certyfikacji muszą zostać dostarczone następujące dane:

1. adres IP lub domenowy urządzenia sieciowego,
2. nazwa jednostki organizacyjnej w której zainstalowane jest urządzenie,

3. adres (zgodny ze standardem SMTP) konta poczty administratora odpowiedzialnego za urządzenie,
4. klucz publiczny wnioskodawcy zawarty w elektronicznym wniosku w formacie PKCS#10,
5. w przypadku rejestracji wniosku zawierającego adres IP lub domenowy nie będący w posiadaniu wnioskodawcy - oświadczenie posiadacza adresu IP lub domenowego o nadaniu prawa używania adresu przez wnioskodawcę.

W trakcie rejestracji weryfikowane są następujące dane:
1. dostęp wnioskodawcy do konta e-mail podanego we wniosku,
2. w przypadku certyfikatów zawierający nazwę domenową - fakt zarejestrowania domeny i jej przynależności do wnioskodawcy,
3. w przypadku certyfikatów zawierających adres IP - możliwość używania adresu IP przez wnioskodawcę – oświadczenie operatora internetowego.

3.2 Wydanie certyfikatu

Termin wydania certyfikatu określa regulamin. Po wydaniu certyfikatu jest on przekazywany posiadaczowi w uzgodniony przez strony sposób.

3.3 Odnowienie certyfikatu

Po okresie ważności certyfikatu subskrybent może złożyć wniosek o wydanie nowego certyfikatu lub odnowienie certyfikatu.

3.4 Akceptacja certyfikatu

Właściciel certyfikatu zobowiązany jest do zweryfikowania poprawności danych zawartych w certyfikacie pod względem zgodności 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 równoważny z potwierdzeniem zgodności danych.
Akceptacja certyfikatu zawierającego niezgodne dane do tych zawartych we wniosku obciąża subskrybenta skutkami używania tego certyfikatu.

3.5 Unieważnienie certyfikatu

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

Warunkiem rozpoczęcia procedury unieważnienia certyfikaty jest poprawna weryfikacja wnioskodawcy.
Unieważnienie certyfikatu jest procedurą NIEODWRACALNĄ.

Procedura składa się z następujących etapów:
- dostarczenie do CCWP podpisanego przez osobę odpowiedzialną wniosku o unieważnienie certyfikatu,
- potwierdzenie wiarygodności osoby podpisującej wniosek i jej odpowiedzialność za określoną usługę.

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 wydania certyfikatu na skutek:
    - fałszerstwa danych zawartych w certyfikacie,
    - niespełnienia istotnych warunków wstępnych do wydania certyfikatu,
    - popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania.

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) to co najmniej 1024 bitów. Para kluczy jest generowana przez wnioskodawcę. Sposób generowania kluczy jest wybierany przez wnioskodawcę. Polityka nie nakłada obowiązku generowania kluczy w bezpiecznym środowisku kryptograficznym. Generowany request musi być w formacie PKCS#10 bez znaków diakrytycznych (polskich znaków).

4.2 Ochrona klucza prywatnego subskrybenta

Za ochronę klucza prywatnego skojarzonego z kluczem publicznym umieszczonym w certyfikacie odpowiedzialny jest wyłącznie posiadacz certyfikatu.

4.3 Aktywacja kluczy

Polityka nie przewiduje wymogów w odniesieniu do sposobu aktywacji klucza prywatnego posiadacza certyfikatu.

4.4 Niszczenie kluczy

Po wygaśnięciu ważności certyfikatu skojarzony z nim klucz prywatny powinien zostać zniszczony, albo dalej przechowywany w taki sposób, aby nie dostał się pod kontrolę nieupoważnionej osoby.

5 Możliwość dostosowania Polityki do wymagań subskrybenta

W przypadkach gdy specyfika świadczonej usługi tego wymaga na pisemny wniosek subskrybenta możliwe są zmiany w profilu certyfikatów:

- zmiana wartości atrybutu keyUsage na wartość podaną w wniosku z wyłączeniem pola keyCertSign i nonRepudiation,
- zmiana wartości rozszerzenia netsacapeCertType na podaną we wniosku,
- zmiana wartości rozszerzenia extendedKeyUsage na podaną we wniosku,
- dodanie nowych typów rozszerzeń podanych w wniosku.